STIC Scientific and Technical Information Center

Search Report EIC 3600

STIC Database Tracking Number: 300338

To: Mamon Obeid
Location: KNX 5A74
Art Unit: 3621
Date: 7/13/2009
Case Serial Number: 10/690911

From: Christian Miner
Location: EIC3600
KNX 4B68
Phone: (571) 272-3010
christian.miner@uspto.gov

Search Notes

Dear Examiner Obeid:

Please find attached the results of your search for the above-referenced case. The search was conducted in Dialog, Proquest, and EBSCOhost.

I have listed *potential* references of interest in the first part of the search results. However, please be sure to scan through the entire report. There may be additional references that you might find useful.

If you have any questions about the search, or need a refocus, please do not hesitate to contact me.

Thank you for using the EIC, and we look forward to your next search!

I. Potential References of Interest

A. Dialog

Dialog eLink: Order File History
13/3K/7 (Item 7 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

00719763

Method and apparatus enabling software trial using an encryption header
Verfahren und Vorrichtung mit einem Verschlusselungskopfteil, die es ermoglicht, Software zu erproben
Methode et appareil permettant de prendre des logiciels a l'essai utilisant un en-tete de chiffrement

Patent Assignee:

- **International Business Machines Corporation;** (200120)
  Old Orchard Road; Armonk, N.Y. 10504; (US)
  (Proprietor designated states: all)

Inventor:

- **Cooper, Thomas Edward**
  858 West Willow Street; Louisville, Colorado 80027; (US)
- **Philips, Hudson Wayne**
  4725 Jameston Street; Boulder, Colorado 80301; (US)
- **Pryor, Robert Franklin**
  7380 Mt. Meeker Road; Longmont, Colorado 80503; (US)

Legal Representative:

- **Duscher, Reinhard, Dr. (94081)**
  IBM Deutschland GmbH, Intellectual Property, Pascalstrasse 100; 70548 Stuttgart; (DE)

	Country	Number	Kind	Date	
Patent	EP	681233	A1	19951108	(Basic)
	EP	681233	B1	20030618	
Application	EP	95105448		19950411	
Priorities	US	235031		19940425	

Designated States:
DE; FR; GB;

International Patent Class (V7): G06F-001/00; G06F-012/14**Abstract Word Count:** 184
NOTE: 29A 29B
NOTE: Figure number on first page: 29A 29B

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	1022
SPEC A	(English)	EPAB95	15201
CLAIMS B	(English)	200325	1224
CLAIMS B	(German)	200325	1145
CLAIMS B	(French)	200325	1348
SPEC B	(English)	200325	13659
Total Word Count (Document A) 16226			
Total Word Count (Document B) 17376			
Total Word Count (All Documents) 33602			

Specification: ...The interfaces allow ordering and unlocking of the software products contained on the distributed media. Unlocking of the software product is accomplished by the reception, **validation**, and recording of a temporary access (**decryption**) **key**.

The file management **program** is resident in the user-controlled **data** processing system and becomes a part of the operating system in the user's computer. An example of such a resident program (in the PC... ...timer can be used to count down a particular predefined period (such as thirty days); alternatively, the counter can be used to decrement through a **predefined number** of trial "sessions" which are allowed during the trial mode of operation. If the key is valid, the file management program communicates directly with the...

Specification: ...The interfaces allow ordering and unlocking of the software products contained on the distributed media. Unlocking of the software product is accomplished by the reception, **validation**, and recording of a temporary access (**decryption**) **key**.

The file management **program** is resident in the user-controlled **data** processing system and becomes a part of the operating system in the user's computer. An example of such a resident program (in the PC... ...timer can be used to count down a particular predefined period (such as thirty days); alternatively, the counter can be used to decrement through a **predefined number** of trial "sessions" which are allowed during the trial mode of operation. If the key is valid, the file management program communicates directly with the...

Dialog eLink: Order File History
13/3K/13 (Item 13 from file: 349)
DIALOG(R)File 349: PCT FULLTEXT

00320485

METHOD FOR SECURELY USING DIGITAL SIGNATURES IN A COMMERCIAL CRYPTOGRAPHIC SYSTEM
PROCEDE PERMETTANT D'UTILISER EN TOUTE SECURITE DES SIGNATURES NUMERIQUES DANS UN SYSTEME DE CHIFFRAGE COMMERCIAL

Patent Applicant/Patent Assignee:

- **BANKERS TRUST COMPANY**;
  ; ;
- **SUDIA Frank W**;
  ; ;
- **SIRITZKY Brian**;
  ; ;

	Country	Number	Kind	Date
Patent	WO	9602993	A2	19960201
Application	WO	95US9076		19950719
Priorities	US	94277438		19940719

Designated States: (All protection types applied unless otherwise stated - for applications 2004+)
Language Publication Language: English
Filing Language:
Fulltext word count: 14898

Claims:

...said digital signature, and wherein a user transaction in said cryptographic system requires verification by a recipient of said user transaction, said verification based on **information** in said digital certificates and requiring said public **key**, a method of controlling access to said public key comprising the steps of: denying access to said public **key**; providing said recipient with at least one **message** containing rules of said system, said rules including maintaining secrecy of said public key; by said recipient, digitally signing said at least one document, by... ...policy in a cryptographic system, said policy requiring controlling access to a public key, said method comprising the steps of: denying access to said public **key**; providing a recipient with a **message** containing rules of said cryptographic system, said rules including maintaining secrecy of said public key; by said recipient, digitally signing said document, by which said... ...document to form a digital agreement; and returning said digital agreement to said certifying authority; in response to said indicating by said user, by said **certifying** authority, activating said **public key** in said secure **device**.6e A method as in any one of ...s status; and each confirm-to transaction by a user.7* A method as in any one of claims 1@5 wherein said rules include **rules** to pay for **use** by said recipient of intellectual property used in creating or operating the system.8* A method as in claim 1 wherein said user transaction is...

11/5/5 (Item 5 from file: 2)
DIALOG(R)File 2: INSPEC

05351065

Title: A software authentication system for information integrity
Author(s): Harn, L.; Hung-Yu Lin; Shoubao Yang
Author Affiliation: Missouri Univ., Kansas City, MO, USA
Journal: Computers & Security , vol.11 , no.8 , pp.747-52
Country of Publication: UK
Publication Date: Dec. 1992
ISSN: 0167-4048
CODEN: CPSEDU
U.S. Copyright Clearance Center Code: 0167-4048/92/$5.00
Language: English
Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: The authors describe a software authentication technique based on the public **key** cryptography for information integrity. The software provider can use a **secret key** to sign any released **program** and the user can **verify** the integrity of **programs** obtained from vendors or a trusted information database. The software provider needs to go through a registration process to become `licensed' and obtains certificates from multiple certificate centers before being able to sign any released **program**. Users need only one **public key** to **verify** the integrity of the **programs** (*13 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: **data** integrity; **message** authentication; **public key** cryptography
Identifiers: software authentication system; **information** integrity; **public key** cryptography; software provider; secret **key**; trusted **information** database; registration process; certificates
Classification Codes: C6130S (Data security)
INSPEC Update Issue: 1993-007

17/3,K/1 (Item 1 from file: 9)
DIALOG(R)File 9: Business
& Industry(R)

01026823
Supplier Number: 23606872 **(USE FORMAT 7 OR 9**
FOR FULLTEXT)
Software 'Signs' Executable Content
(
Authenticode was recently launched by Microsoft; software provides method of
'signing' executable content with public and private keys)

Information Week , p 32

August 12, 1996
Document Type: Journal
ISSN: 8750-6874 (United States)
Language:
English **Record Type:** Fulltext
Word Count:
116

TEXT:
Authenticode, the microsoft software that provides a method of "signing" executable **content** with public and private keys, was introduced last week. The **digital-signature** approach is similar to **public-key** encryption techniques and lets Web browsers **validate** the source and **authenticity** of downloadable content.

The **product** uses VeriSign Inc."s Digital **ID** 128-bit signatures to authenticate executable content in real time.

Any program, Java applet, dynamic link library, or ActiveX control can be digitally signed by...

21/3,K/16 (Item 1 from file: 636)
DIALOG(R)File 636: Gale Group Newsletter DB(TM)

02868850 **Supplier Number:** 45822377 **(USE FORMAT 7 FOR FULLTEXT)**

Key Escrow Nitty Gritty: How the Criteria would be Implemented
Export Practitioner , v 9 , n 9 , p N/A
Sept 30 , 1995
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal ; Trade
Word Count: 1168

...to the number of bits needed to decrypt a message which are not available over the communications channel. For some encryption algorithms the key is **defined** to be a **number** of bits which are kept secret and a number of bits which are transmitted in the clear (message key / initialization vector / salt). This criterion only **specifies** the **number** of secret bits.

2.The product shall be designed to prevent multiple encryption (e.g. triple-DES).

One way to do this would be for...

...disabled.

If one follows the steps under criterion #3, a receiving program could verify the escrow certificate contained in the message header, extract the escrow **public key,** and **verify** that the encrypted message **decryption key** is also found in the header. If it is not there, decryption does not proceed.

7.The key escrow mechanism allows access to user's...

...with #10.

Following the example in criterion #3, the software could accept the load of a new escrow certificate. The software could store a '"root" **public key** which is used to **verify** a certificate containing the escrow agent **public key** which in turn is used to sign the individual user's escrow certificate. Hence, the header might contain both the escrow agent

B. Additional Resources Searched

Financial Times FullText (via ProQuest): No relevant results.

Internet & Personal Computing Abstracts (via EBSCOhost): No relevant results.

II. Inventor Search Results from Dialog

Dialog eLink: Order File History
21/5/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009041623 *Drawing available*
WPI Acc no: 1998-599611/199851
XRPX Acc No: N1998-467001
Audio and video data communication method - involves using controller which accepts transmitted data, only when its random security ID number corresponds with specific pre-generated random number at reception side
Patent Assignee: SONY CORP (SONY)
Inventor: FUKAMI T; **MAARI K**

Patent Family (1 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 10269290	A	19981009	JP 199774183	A	19970326	199851	B

Priority Applications (no., kind, date): JP 199774183 A 19970326

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
JP 10269290	A	JA	36	40	

Alerting Abstract JP A
The method involves generating a random number as a security ID by using a security ID generator (19), during data communication.The random number is added to the transmission data. At the reception side, the random number of the transmitted data is compared with a pre-generated random number. A controller (16) accepts the received data when the random numbers are in accord.
ADVANTAGE - Prevents impersonating in case of communication of simple money supplement data.

Title Terms /Index Terms/Additional Words: AUDIO; VIDEO; DATA; COMMUNICATE; METHOD; CONTROL; ACCEPT; TRANSMIT; RANDOM; SECURE; ID; NUMBER; CORRESPOND; SPECIFIC ; PRE; GENERATE; RECEPTION; SIDE

Class Codes

Dialog eLink: Order File History
23/5/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0012442877 *Drawing available*
WPI Acc no: 2002-388427/200242
XRPX Acc No: N2002-304409
Information processor for PDA transmits stored digital video broadcasted program data to mobile telephone, based on demand
Patent Assignee: SONY CORP (SONY)
Inventor: **MAARI K**

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type

JP 2002077839	A	20020315	JP 2000253334	A	20000824	200242	B

Priority Applications (no., kind, date): JP 2000253334 A 20000824

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
JP 2002077839	A	JA	21	28	

Alerting Abstract JP A
NOVELTY - A receiver (111) of a video recording server (11) receives the digital **video** broadcast program which is then **encoded** and stored in a memory (114). Based on the demand from the mobile telephone (50), the stored data are transmitted. DESCRIPTION - INDEPENDENT CLAIMS are also included for the following:

A. Information processing system;
B. Information processing method;
C. Recorded medium storing information processing program

USE - For transmission of digital television broadcast program, information from digital versatile disk player to mobile telephone such as personal digital assistant.
ADVANTAGE - The broadcast program is viewed and listened reliably using mobile telephone.
DESCRIPTION OF DRAWINGS - The figure shows the components of the network system with image processing apparatus. (Drawing includes non-English language text).
11 Video recording server
50 Mobile telephone
111 Receiver
114 Memory

Title Terms /Index Terms/Additional Words: INFORMATION; PROCESSOR; TRANSMIT; STORAGE; DIGITAL; VIDEO; PROGRAM; DATA; MOBILE; TELEPHONE; BASED; DEMAND

Class Codes

File Segment: EPI;
DWPI Class: T01; W02; W04
Manual Codes (EPI/S-X): T01-J10D; T01-J10G; T01-M06A1A; T01-N01D1B; T01-S03; W02-C03C; W02-D05C; W04-C10A2

Dialog eLink: Order File History
23/5/2 (Item 2 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0009041622 *Drawing available*
WPI Acc no: 1998-599610/199851
XRPX Acc No: N1998-467000
Digital database distribution management method - involves computing service fee information using decoded utilisation information based on which service fee allocation is carried out

Patent Assignee: SONY CORP (SONY)
Inventor: **MAARI K**

Patent Family (5 patents, 2 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
JP 10269289	A	19981009	JP 199774182	A	19970326	199851	B
US 20040073451	A1	20040415	US 199846693	A	19980324	200426	E
			US 2003690911	A	20031022		
US 20040107167	A1	20040603	US 199846693	A	19980324	200436	E
			US 2003690747	A	20031022		
US 7120604	B2	20061010	US 199846693	A	19980324	200667	E
			US 2003690747	A	20031022		
JP 3994466	B2	20071017	JP 199774182	A	19970326	200770	E

Priority Applications (no., kind, date): JP 199774182 A 19970326

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
JP 10269289	A	JA	39	40		
US 20040073451	A1	EN			Division of application	US 199846693
US 20040107167	A1	EN			Division of application	US 199846693
US 7120604	B2	EN			Division of application	US 199846693
JP 3994466	B2	JA	52		Previously issued patent	JP 10269289

Alerting Abstract JP A
The method involves encrypting digital data using specific encryption key. The encrypted data is transmitted to requested party based on the received transmission demand. The encrypted data is decoded using the encryption key and is transmitted. The billing information corresponding to the utilised digital data for every user is determined based on the transmitted data. The determined billing information is then transmitted to the corresponding user. The utilisation information received by user is judged and decoded. The service fee for the utilised information to be collected from the respective user is determined based on the decoded data. Then allocation of service fee is carried out.
ADVANTAGE - Prevents copy or unauthorised usage of digital data.

Title Terms /Index Terms/Additional Words: DIGITAL; DATABASE; DISTRIBUTE; MANAGEMENT; METHOD; COMPUTATION; SERVICE; FEE; INFORMATION; DECODE; UTILISE; BASED; ALLOCATE; CARRY

Class Codes

Dialog eLink: Order File History
23/5/3 (Item 1 from file: 347)
DIALOG(R)File 347: JAPIO

07209407 **Image available**
INFORMATION PROCESS AND PROCESSING METHOD, AND MEDIUM WITH PROGRAM STORED THEREIN

Pub. No.: 2002-077839 [JP 2002077839 A]

Published: March 15, 2002 (20020315)
Inventor: MAARI KOUICHI
Applicant: SONY CORP
Application No.: 2000-253334 [JP 2000253334]
Filed: August 24, 2000 (20000824)
International Class: H04N-007/14; G06F-017/60; H04N-005/44; H04N-005/445; H04N-007/24; H04N-007/173

ABSTRACT

PROBLEM TO BE SOLVED: To make possible to view a digital broadcast even on a potable information terminal.

SOLUTION: In a digital portable telephone 50 with camera, an image recording server 11 is designated to record a program of digital broadcast. The image recording server 11 receives a designated program through a receiver 11, decodes it through a decoder 112 and encodes it through an encoder 113 suitably for the digital portable telephone 50 with camera. **Encoded content** data is stored in a storage unit 114. When a user views a recorded program, the user request the image recording server 11. In response to the request, the image recording server 11 reads out a requested content data from the storage unit 114 and delivers it to the digital portable telephone 50 with camera.

00677495

Non-volatile memory device
Nichtfluchtige Halbleiteranordnung
Dispositif de memoire remanente

Patent Assignee:

- **SONY CORPORATION**; (214021)
  7-35 Kitashinagawa 6-chome Shinagawa-ku; Tokyo 141; (JP)
  (Proprietor designated states: all)

Inventor:

- **Arase, Kenshiro, c/o SONY CORPORATION**
  7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)
- **Maari, Koichi, c/o SONY CORPORATION**
  7-35, Kitashinagawa 6-chome; Shinagawa-ku, Tokyo; (JP)
- **...JP)**
  ; ;
- **Maari, Koichi, c/o SONY CORPORATION...**
  ; ;

Legal Representative:

- **Thevenet, Jean-Bruno et al (39781)**
  Cabinet Beau de Lomenie 158, rue de l'Universite; 75340 Paris Cedex 07; (FR)

	Country	Number	Kind	Date	
Patent	EP	649172	A2	19950419	(Basic)
	EP	649172	A3	19951025	
	EP	649172	B1	20020102	
Application	EP	94402301		19941014	
Priorities	JP	93258711		19931015	
	JP	93264639		19931022	

Designated States:
DE; FR; IT;

International Patent Class (V7): H01L-027/115; H01L-021/8247**Abstract Word Count:** 73
NOTE: 5
NOTE: Figure number on first page: 5

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	EPAB95	217
SPEC A	(English)	EPAB95	5469
CLAIMS B	(English)	200201	99
CLAIMS B	(German)	200201	85
CLAIMS B	(French)	200201	130
SPEC B	(English)	200201	2843
Total Word Count (Document A) 5687			
Total Word Count (Document B) 3157			
Total Word Count (All Documents) 8844			

III. Text Search Results from Dialog

A. Patent Files, Abstract

```
File 350:Derwent WPIX 1963-2009/UD=200943
         (c) 2009 Thomson Reuters
File 347:JAPIO Dec 1976-2009/Mar(Updated 090708)
         (c) 2009 JPO & JAPIO


Set     Items   Description
S1       2153   (CONFIRM??? OR CONFIRMATION OR ACKNOWLEDG??? OR ACKNOWLEDGEMENT OR
AFFIRM??? OR ATTEST??? OR CERTIFY??? OR CHECK??? OR SUBSTANTIAT??? OR VERIFY??? OR
PROVE? ? OR PROVING OR VALIDAT??? OR AUTHENTICITY) (10N) ((PUBLIC OR PRIVATE OR
SYSTEM OR SECRET OR SYMMETRIC OR SYNCHRONOUS OR CONTENT OR ASSESS OR DECRYPTION OR
ASYMMETRIC OR SYMMETRIC)()KEY? ? OR PKI OR PGP OR WEB()TRUST)

S2   11753938   S1 (5N) PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR
DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR
DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR
WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?

S3     186403   USAGE (3N) (CONDITIONS OR TERMS OR RULES OR RESTRICTIONS OR RIGHTS
OR LIMITATIONS) OR (LIMIT??? OR RESTRICT??? OR SPECIFI?? OR PERMITTED OR FIXED OR
DEFINED OR STIPULATED OR PREDEFINED OR PRESET OR PREESTABLISHED OR PREDETERMINED)
(3N) (NUMBER OR TIMES OR COPIED OR COPIES OR PLAYED OR DOWNLOAD??) OR
AVAILABILITY()DATES OR USAGE()PERIODS

S4      61216   (CRYPTOGRA? OR (ELECTRONIC OR DIGITAL)()(SEAL? ? OR SIGNATURE? ? OR
CERTIFICAT??? OR ENVELOPE? ?) OR ENCRYPT??? OR CIPHER? ? OR CYPHER? ? OR HASH?? OR
ENCOD??? OR ENC?PHER??) (5N) (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR
ART OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR
PHOTOGRAPH OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS
OR ALBUM OR ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S5     226155   (UNENCOD??? OR UNCOD??? OR UNENCRYPT??? OR DECRYPT??? OR DECOD???
OR DEC?PHER??? OR KEY OR KEYS) (5N) (MESSAGE? ? OR SIGNAL? ? OR PACKET? ? OR
TRANSMISSION? ? OR BLOCK? ? OR INFORMATION OR DATA)

S6     151087   (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR
ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR
PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR AUDIOVISUAL OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR PRODUCT OR UNIQUE) (3N)
(ID OR IDS OR IDENTIFICATION OR NUMBER? ? OR IDENTIFIER? ?)

S7        117   AU=(MAARI, K? OR MAARI K? OR MAARI (1N) (K OR KOICHI))
S8    1554519   IC=G06F
S9        541   S1 (5N) (PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR
DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR
DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR
WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?)
```

```
S10          19    S9 AND S3
S11          15    S10 AND (S4 OR S5 OR S6)
S12          56    S9 AND S4
S13          43    S12 AND S5
S14           9    S13 AND S6
S15           7    S14 NOT S11
S16           1    S15 NOT AY>1997
S17          88    S9 NOT AY>1997
S18          38    S17 AND S8
S19           6    S18 AND (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART
OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH
OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S20           0    S7 AND S1
S21           1    S7 AND S3
S22           3    S7 AND S4
S23           3    S22 NOT S21
```

Dialog eLink: Order File History
11/5/13 (Item 13 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0007786419 *Drawing available*
WPI Acc no: 1996-412885/199642
Related WPI Acc No: 1998-009147; 1998-179618; 1998-193856; 1998-261976; 2002-225639; 2002-462772; 2004-050631; 2005-252363; 2006-605130; 2007-081309
Secure content delivery method for electronic transaction - involves encapsulating and encrypting digital information within containers and delivering them to user in protected environment
Patent Assignee: ELECTRONIC PUBLISHING RESOURCES INC (ELPU-N); GINTER K L (GINT-I); INTERTRUST TECH CORP (INTE-N); INTERTRUST TECHNOLOGIES CORP (INTE-N); SHEAR V H (SHEA-I); SHEAR V M (SHEA-I); SPAHN F J (SPAH-I); VAN WIE D M (VWIE-I); INTERTRUST TECNOLOGIES CORP (INTE-N)
Inventor: GINTER K; GINTER K L; SHEAR V; SHEAR V H; SHEAR V M; SIBERT O W; SPAHN F; SPAHN F J; VAN W D M; VAN WIE D; VAN WIE D M; WEBER R P; WIE D; WIE D M V ; HILL V H

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 5915019	A	19990622	US 1995388107	A	19950213	199931	E
US 5917912	A	19990629	US 1995388107	A	19950213	199932	E
WO 9627155	A2	19960906	WO 1996US3303	A	19960213	199642	B
AU 9649266	A	19960918	AU 1996049266	A	19960213	199701	E
US 5920876	A	19990706	US 1995388107	A	19950213	199937	E
EP 861461	A2	19980902	EP 1996902731	A	19960213	199839	E
US 5982891	A	19991109	US 1995388107	A	19950213	199954	E
JP 10512074	W	19981117	JP 1996526318	A	19960213	199905	E
			WO 1996US2303	A	19960213		
US 5910987	A	19990608	US 1995388107	A	19950213	199930	E
			US 1996760440	A	19961204		

Priority Applications (no., kind, date): US 1995388107 A 19950213; US 199617722 P 19960515; US 199618132 P 19960522; US 1996689606 A 19960812; US 1996689754 A 19960812; US 1996699711 A 19960812; US 1996699712 A 19960812; WO 1996US14262 A 19960904; US 1996760440 A 19961204; US 1997778256 A 19970108; US 1997780393 A 19970108; US 1997780545 A 19970108; US 199737931 P 19970214; US 1997964333 A 19971104; US 1998208017 A 19981209; US 1998221479 A 19981228; US 1999247328 A 19990210; US 1999327405 A 19990607; US 1999328668 A 19990609; US 1999328671 A 19990609; US 1999335465 A 19990617; US 1999342899 A 19990629; US 1999389967 A 19990903; US 1999398665 A 19990917; US 2000632944 A 20000804; US 2000678252 A 20001003; US 2000698044 A 20001030; US 2001764370 A 20010119; US 2001790566 A 20010223; US 2001870801 A 20010601; US 2002106742 A 20020325; US 2002157061 A 20020530; US 2002189231 A 20020705; US 2003607562 A 20030625; US 2003618427 A 20030710; US 2003696659 A 20031028; US 200590982 A 20050324; US 2005102514 A 20050407; US 2005231355 A 20050920; US 2006359979 A 20060221; US 2006405130 A 20060413; US 2006412348 A 20060426; US 2006438953 A 20060522; US 2006440141 A 20060523; US 2006505778 A 20060816; US 2007807313 A 20070525; US 2007807342 A 20070525; US 2007821862 A 20070625; US 2007879006 A 20070712; US 2007827983 A 20070713; US 2007827996 A 20070713; US 2007827997 A 20070713; US 2007829553 A 20070727; US 2007894329 A 20070820; US 2007894538 A 20070820; US 2007980075 A 20071029; US 2007980245 A 20071029; US 2007980282 A 20071029; US 2007981297 A 20071030; US 2007981332 A 20071030; US 2007981465 A 20071030; US 2007981791 A 20071030; US 2007981816 A 20071030; US 2008259243 A 20081027

Alerting Abstract WO A2
The method involves encapsulating digital information within one or more digital containers. At least one portion of the information is encrypted. At least partially secure control information is associated for managing interaction with the encrypted digital information and/or the digital container.
One or more of the digital containers are delivered to a digital information user. A protected processing environment is employed to securely control decryption of at least a portion of the digital information.
ADVANTAGE - Provides secure chain of handling and control.

Title Terms /Index Terms/Additional Words: SECURE; CONTENT; DELIVER; METHOD; ELECTRONIC ; TRANSACTION; ENCAPSULATE; DIGITAL; INFORMATION; CONTAINER; USER; PROTECT; ENVIRONMENT

Dialog eLink: Order File History
11/5/15 (Item 15 from file: 350)
DIALOG(R)File 350: Derwent WPIX
(c) 2009 Thomson Reuters. All rights reserved.

0007265455
WPI Acc no: 1995-322197/199542
XRPX Acc No: N1995-242487; N1997-003248
Information dissemination control system - has information structured logically to incorporate usage history and allowable access window before encryption into header and body portions
Patent Assignee: INST SYSTEMS SCI (SYST-N); UNIV SINGAPORE NAT (UYSI-N)
Inventor: ALCOTT D N; KANKANHALLI M S; MOHAN S K; NARASIMHALU A D; UEIGUO W; WANG W

		Patent Family (10 patents, 2 countries)			19950313		
Patent Number	**Kind**	**Date**	**Application Number**	**Kind**	**Date**	**Update**	**Type**
EP 672991	A2	19950920	EP 1995301630	A	19950313	199542	B
US 5499298	A	19960312	US 1994210174	A	19940317	199616	E
JP 8272743	A	19961018	JP 199559425	A	19950317	199701	NCE
EP 672991	A3	19961127	EP 1995301630	A	19950313	199702	E
EP 672991	B1	19980520	EP 1995301630	A	19950313	199824	E
DE 69502526	E	19980625	DE 69502526	A	19950313	199831	E

Priority Applications (no., kind, date): US 1994210174 A 19940317; JP 199559425 A 19950317

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes
EP 672991	A2	EN	22		
Regional Designated States,Original	DE GB				
US 5499298	A	EN	20		
JP 8272743	A	JA	19	13	
EP 672991	A3	EN			
EP 672991	B1	EN			
Regional Designated States,Original	DE GB				
DE 69502526	E	DE			Application EP 1995301630
					Based on OPI patent EP 672991

Alerting Abstract EP A2

The appts controls the dissemination of digital information. Digital information is structured logically to incorporate usage history and allowable access window before it is encrypted in a header and a body. The end user accesses the digital information with a tamper-proof controlled **information** access device by **decrypting** the digital **information**.

A controller disposed in the controlled information access device permits end users to access transparently uncontrolled information. Controlled digital information will be accessed as long as the conditions specified by the information provider are met. The controlled information may be disseminated in either an on-line or off-line manner.

USE/ADVANTAGE - Provides transparent access to uncontrolled digital information together with controlled digital information with same access appts.

Title Terms /Index Terms/Additional Words: INFORMATION; DISSEMINATE; CONTROL; SYSTEM; STRUCTURE; LOGIC; INCORPORATE; HISTORY; ALLOW; ACCESS; WINDOW; ENCRYPTION; HEADER; BODY; PORTION

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-0015/00	C	I	Main	R	20060101"
G06F-017/60	C	I	Secondary	R	20060101"
G06F-007/02	C	I		R	20060101
G06F-0009/06	C	I	L	R	20060101
G06F-0021/00	C	I		R	20060101
G06F-0021/20	C	I	L	R	20060101
H04L-0009/00	C	I		R	20060101
H04L-0009/10	C	I		R	20060101
H04L-0009/32	C	I	L	R	20060101
H04N-0007/167	C	I		R	20060101
H04L-0009/10	A	I		R	20060101
H04L-0009/12	A	I		R	20060101

ECLA: G07F-017/16, H04N-007/167D
US Classification, Issued: 38025, 3809, 38021, 38023, 38030, 38049

Dialog eLink: Order File History
16/5/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0007075711 *Drawing available*
WPI Acc no: 1995-099929/199514
XRPX Acc No: N1995-078977
Document class verification method - verifies documents to assure that information in documents is authenticated and unchanged, documents may be identification cards containing both text and image of bearer and encryption information
Patent Assignee: PITNEY BOWES INC (PITB)
Inventor: BERSON W

Patent Family (6 patents, 5 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
EP 640946	A1	19950301	EP 1994306218	A	19940823	199514	B
CA 2130531	A	19950224	CA 2130531	A	19940819	199521	E
US 5426700	A	19950620	US 1993110268	A	19930823	199530	E
EP 640946	B1	19990203	EP 1994306218	A	19940823	199910	E
DE 69416360	E	19990318	DE 69416360	A	19940823	199917	E
			EP 1994306218	A	19940823		
CA 2130531	C	20000125	CA 2130531	A	19940819	200025	E

Priority Applications (no., kind, date): US 1993110268 A 19930823

Patent Details

Patent Number	Kind	Lan	Pgs	Draw	Filing Notes	
EP 640946	A1	EN	13	4		
Regional Designated States,Original	DE FR GB NL					
CA 2130531	A	EN				
US 5426700	A	EN	11	4		
EP 640946	B1	EN				
Regional Designated States,Original	DE FR GB NL					
DE 69416360	E	DE			Application	EP 1994306218
					Based on OPI patent	EP 640946
CA 2130531	C	EN				

Alerting Abstract EP A1
The method provides enabling information for enabling the retrieval of a decryption key from any document in a selected group of class of documents. It is determined if the document is indeed in the selected group. If it is, it retrieves the decryption key (Di) from the document.
The encrypted **information** (Ei[M]) is **decrypted** to obtain the **decrypted information** (Di[Ei[M]]) from which the information (M) is then derived from the document. The **decrypted** encrypted **information** is compared with the information

(M) to verify the information contained in the document as being authentic and unchanged.
ADVANTAGE - Provides for easy method of verification of document, such as driving licence or similar when presented as proof of identity by bearer.

Title Terms /Index Terms/Additional Words: DOCUMENT; CLASS; VERIFICATION; METHOD; ASSURE; INFORMATION; AUTHENTICITY; UNCHANGED; IDENTIFY; CARD; CONTAIN; TEXT ; IMAGE; BEAR; ENCRYPTION

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G07F-007/12			Main		"Version 7"
G07D-0007/00	A	I		R	20060101
G07D-0007/20	A	I		R	20060101
G07F-0007/12	A	I		R	20060101
G07D-0007/00	C	I		R	20060101
G07F-0007/12	C	I		R	20060101

ECLA: G07D-007/00B8, G07D-007/20, G07F-007/08E4
US Classification, Issued: 38023, 38051, 38030
File Segment: EPI;
DWPI Class: T05
Manual Codes (EPI/S-X): T05-H02C

Dialog eLink: Order File History
19/5/1 (Item 1 from file: 350)
DIALOG(R)File 350: Derwent WPIX

0012406571 *Drawing available*
WPI Acc no: 2002-350655/200238
Related WPI Acc No: 1999-560197
XRPX Acc No: N2002-275472
Digital content transformation method in consumer electronic device, involves establishing preliminary control channel when exchanged hashed random challenges match expected values
Patent Assignee: AUCSMITH D W (AUCS-I); INTEL CORP (ITLC); TRAW C B S (TRAW-I)
Inventor: AUCSMITH D W; TRAW C B S

Patent Family (2 patents, 1 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
US 20020007452	A1	20020117	US 1997791245	A	19970130	200238	B
			US 1997909338	A	19970811		
US 6542610	B2	20030401	US 1997909338	A	19970811	200324	E

Priority Applications (no., kind, date): US 1997791245 A 19970130; US 1997909338 A 19970811

US 20020007452	A1	EN	20P	Cont Details of application	US 1997791245
Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	C-I-P of patent	**Filing Notes**	US 5949877

Alerting Abstract US A1
NOVELTY - The random challenges which are exchanged between the two consumer electronic devices, are encrypted with secret key and are hashed. The hashed random challenges are exchanged and are compared with expected value. The digital **content** is transferred over a preliminary control channel which is established, when hashed random challenge match the expected value.
USE - For transferring digital **audio/video content** between consumer electronic (CE) devices such as **DVD** player/recorder, digital television, set-top boxes, digital satellite service receivers as well as applications running on computers through IEEE 1394 bus, Ethernet, asynchronous transfer mode (**ATM**) network, cable television system, telephony network.
ADVANTAGE - Allows for high level of **content** protection for consumer electronics equipment and computer systems.
DESCRIPTION OF DRAWINGS - The figures show the flow diagram of the authentication and preliminary control channel key generation.

Title Terms /Index Terms/Additional Words: DIGITAL; **CONTENT**; TRANSFORM; METHOD; CONSUME; ELECTRONIC; DEVICE; ESTABLISH; PRELIMINARY; CONTROL; CHANNEL; EXCHANGE; HASH; RANDOM; MATCH; VALUE

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G06F-0001/00	A	N		R	20060101
G06F-0021/00	A	I		R	20060101
G11B-0020/00	A	I		R	20060101
H04L-0012/64	A	N		R	20060101
H04L-0009/32	A	I		R	20060101
G06F-0001/00	C	N		R	20060101
G06F-0021/00	C	I		R	20060101
G11B-0020/00	C	I		R	20060101
H04L-0012/64	C	N		R	20060101
H04L-0009/32	C	I		R	20060101

ECLA: G06F-021/00N5A4, G06F-021/00N7D, G11B-020/00P, H04L-009/32T, H04L-012/40F8
ICO: S06F-211:014B
US Classification, Current Main: 713-152000; Secondary: 380-201000, 705-057000
US Classification, Issued: 713152, 380201, 70557, 380262, 380260, 380264, 713168, 713169
File Segment: EPI;
DWPI Class: T01; W01; W02; W03; W04
Manual Codes (EPI/S-X): T01-D01; T01-N02B1B; W01-A05A; W01-A06B5A; W02-F03; W03-A16C3; W04-P01A

0008702847 *Drawing available*
WPI Acc no: 1998-243135/199822
XRPX Acc No: N1998-192458

Encrypted communication system for limiting damage caused by leaked key - distributes pair of keys on sub-group basis to receivers and alternates which key is currently relevant for use, for decrypting received signal

Patent Assignee: MATSUSHITA DENKI SANGYO KK (MATU); MATSUSHITA ELECTRIC IND CO LTD (MATU); TOSHIBA CORP (TOKE); TOSHIBA KK (TOKE); TOSHIBA MICROELECTRONICS CORP (TOSZ); Toshiba KK (TOKE)

Inventor: ENDO N; ENDOH N; FUKUSHIMA Y; HIRAYAMA K; KATO T; MAKOTO T; TAKEHISA K; TATEBAYASHI M; YOSHIHISA F

Patent Family (12 patents, 28 countries)

Patent Number	Kind	Date	Application Number	Kind	Date	Update	Type
EP 840476	A2	19980506	EP 1997307629	A	19970929	199822	B
JP 10210025	A	19980807	JP 1997296513	A	19971029	199842	E
KR 1998033369	A	19980725	KR 199756940	A	19971031	199932	E
TW 370661	A	19990921	TW 1997115448	A	19971020	200036	E
US 6151394	A	20001121	US 1997940052	A	19970930	200101	E
CN 1184386	A	19980610	CN 1997121562	A	19971030	200254	E
JP 3526522	B2	20040517	JP 1997296513	A	19971029	200433	E
KR 426460	B	20040616	KR 199756940	A	19971031	200468	E
EP 840476	B1	20050817	EP 1997307629	A	19970929	200555	E
DE 69733986	E	20050922	DE 69733986	A	19970929	200564	E
			EP 1997307629	A	19970929		
DE 69733986	T2	20060126	DE 69733986	A	19970929	200611	E
			EP 1997307629	A	19970929		
CN 1192544	C	20050309	CN 1997121562	A	19971030	200634	E

Priority Applications (no., kind, date): JP 1996290373 A 19961031; EP 1997307629 A 19970929

DE 69733986	T2	DE	Patent Detail		Application	EP 1997307629
Patent Number	**Kind**	**Lan**	**Pgs**	**Draw**	Based on OPI patent	**Filing Note** EP 840476
EP 840476	A2	EN	20	8		
Regional Designated States,Original	AL AT BE CH DE DK ES FI FR GB GR IE IT LI LT LU LV MC NL PT RO SE SI					
JP 10210025	A	JA	13	8		
KR 1998033369	A	KO		8		
TW 370661	A	ZH				
JP 3526522	B2	JA	14		Previously issued patent	JP 10210025
KR 426460	B	KO			Previously issued patent	KR 98033369
EP 840476	B1	EN				
Regional Designated States,Original	DE FR GB					
DE 69733986	E	DE			Application	EP 1997307629
					Based on OPI patent	EP 840476

Alerting Abstract EP A2
The communication system has a single transmitter sending signals to a number of receiver stations, e.g. encoded cable television signals. The transmissions may be encrypted requiring the receivers to hold a decrypting key. The receivers are arranged in sub-groups and each sub-group has a pair of security keys from a larger key set distributed to it.
A transmission to a sub-group is encrypted with one of the keys. The receiver decrypts the transmission using both keys and uses a test to determine the correct decryption. The relevant key is then used for further decryption. The test algorithm can be distributed in an encrypted form.
ADVANTAGE - Limits damage caused by leaked keys by operating in sub-groups. Improves security levels by using alternating keys.

Title Terms /Index Terms/Additional Words: ENCRYPTION; COMMUNICATE; SYSTEM; LIMIT; DAMAGE; CAUSE; LEAK; KEY; DISTRIBUTE; PAIR; SUB; GROUP; BASIS; RECEIVE; ALTERNATE; CURRENT; RELEVANT; SIGNAL

Class Codes

International Patent Classification

IPC	Class Level	Scope	Position	Status	Version Date
G09C-001/00; H04L-009/00; H04L-009/08			Main		"Version 7"
G06F-0012/14	A	I	L	R	20061008
G06F-0021/24	A	I	L	R	20060101
G09C-0001/00	A	I	L	R	20060101
H04L-0009/08	A	I	F	R	20060101
H04L-0009/08	A	I	F		20060101
H04L-0009/08	A	I		R	20060101
H04L-0009/14	A	I	L	R	20060101
G06F-0012/14	C	I	L	R	20060101
G06F-0021/00	C	I	L	R	20060101
G09C-0001/00	C	I	L	R	20060101
H04L-0009/08	C	I	F	R	20060101
H04L-0009/08	C	I		R	20060101
H04L-0009/14	C	I	L	R	20060101

ECLA: H04L-009/08B2
US Classification, Current Main: 380-283000; Secondary: 380-043000, 380-277000, 380-278000
US Classification, Issued: 380283, 380278, 380277, 38043

File Segment: EngPI; EPI;
DWPI Class: W01; P85
Manual Codes (EPI/S-X): W01-A05A

B. Patent Files, Full-Text

```
File 348:EUROPEAN PATENTS 1978-200928
         (c) 2009 European Patent Office
File 349:PCT FULLTEXT 1979-2009/UB=20090709|UT=20090702
         (c) 2009 WIPO/Thomson


Set     Items   Description
S1       5922   (CONFIRM??? OR CONFIRMATION OR ACKNOWLEDG??? OR ACKNOWLEDGEMENT OR
AFFIRM??? OR ATTEST??? OR CERTIFY??? OR CHECK??? OR SUBSTANTIAT??? OR VERIFY??? OR
PROVE? ? OR PROVING OR VALIDAT??? OR VALIDITY OR AUTHENTICITY) (10N) ((PUBLIC OR
PRIVATE OR SYSTEM OR SECRET OR SYMMETRIC OR SYNCHRONOUS OR CONTENT OR ASSESS OR
DECRYPTION OR ASYMMETRIC OR SYMMETRIC)()KEY? ? OR PKI OR PGP OR WEB()TRUST)

S2       1498   S1 (5N) (PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR
DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR
DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR
WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?)

S3     369803   (USAGE OR USE) (3N) (CONDITION? ? OR TERMS OR RULE? ? OR
RESTRICTION? ? OR RIGHTS OR LIMITATION? ?) OR (LIMIT??? OR RESTRICT??? OR SPECIFI??
OR PERMITTED OR FIXED OR DEFINED OR STIPULATED OR PREDEFINED OR PRESET OR
PREESTABLISHED OR PREDETERMINED) (3N) (NUMBER OR TIMES OR COPIED OR COPIES OR
PLAYED OR DOWNLOAD??) OR AVAILABILITY()DATES OR USAGE()PERIODS

S4       97223   (CRYPTOGRA? OR (ELECTRONIC OR DIGITAL)()(SEAL? ? OR SIGNATURE? ? OR
CERTIFICAT??? OR ENVELOPE? ?) OR ENCRYPT??? OR CIPHER? ? OR CYPHER? ? OR HASH?? OR
ENCOD??? OR ENC?PHER??) (10N) (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR
ART OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR
PHOTOGRAPH OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS
OR ALBUM OR ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S5      196876   (UNENCOD??? OR UNCOD??? OR UNENCRYPT??? OR DECRYPT??? OR DECOD???
OR DEC?PHER??? OR KEY OR KEYS) (10N) (MESSAGE? ? OR SIGNAL? ? OR PACKET? ? OR
TRANSMISSION? ? OR BLOCK? ? OR INFORMATION OR DATA)

S6      351791   (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR
ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR
PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR AUDIOVISUAL OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR PRODUCT OR UNIQUE OR
SECURITY OR DIGITAL) (5N) (ID OR IDS OR IDENTIFICATION OR NUMBER? ? OR IDENTIFIER?
?)

S7          1   AU=(MAARI, K? OR MAARI K? OR MAARI (1N) (K OR KOICHI))
S8     232239   IC=G06F
S9         63   S2 (S) S3
S10        46   S9 (S) (S4 OR S5 OR S6)
S11        13   S10 NOT AY>1997
S12        13   IDPAT (sorted in duplicate/non-duplicate order)
S13        13   IDPAT (primary/non-duplicate records only)
S14        16   S2 (10N) S3
```

```
S15          12    S14 NOT S13
S16           4    S15 NOT AY>1997
```

Dialog eLink: Order File History
13/3K/1 (Item 1 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

02059858

Systems and methods for secure transaction management and electronic rights protection
System und Verfahren fur sichere Transaktionsverwaltung und elektronischen Rechteschutz
Systemes et procedes de gestion de transactions securisees et de protection des droits electroniques

Patent Assignee:

- **Intertrust Technologies Corporation**; (7330020)
  955 Stewart Drive; Sunnyvale, CA 94085-3913; (US)
  (Applicant designated States: all)

Inventor:

- **Ginter, Karl L.**
  10404 43rd Avenue; Beitsville, MD 20705; (US)
- **Shear, Victor H.**
  5203 Battery Lane; Bethesda, MD 20814; (US)
- **Spahn, Francis J.**
  2410 Edwards Avenue; El Cerrito, CA 94530; (US)
- **Van Wie, David M.**
  1250 Lakeside Drive; Sunnyvale, CA 94086; (US)

Legal Representative:

- **Garner, Jonathan Charles Stapleton et al (9222071)**
  FJ Cleveland 40-43 Chancery Lane; London WC2A 1JQ; (GB)

	Country	Number	Kind	Date	
Patent	EP	1662418	A2	20060531	(Basic)
	EP	1662418	A3	20060726	
Application	EP	2006075503		19960213	
Priorities	US	388107		19950213	

Designated States:
AT; BE; CH; DE; DK; ES; FR; GB; GR; IE;
IT; LI; LU; MC; NL; PT; SE;

Extended Designated States:
AL; LT; LV; SI;

Related Parent Numbers: Patent (Application):EP 861461 (EP 96922371)

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0001/00	A	I	F	B	20060101	20060616	H	EP

Abstract Word Count: 165
NOTE: 1
NOTE: Figure number on first page: 1

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability	Available Text	Language	Update	Word Count
CLAIMS A		(English)	200622	302
SPEC A		(English)	200622	193789
Total Word Count (Document A) 194124				
Total Word Count (Document B) 0				
Total Word Count (All Documents) 194124				

Specification: ...602 provides the following RPC based service providers/requestors (each of which have an RPC interface or "RSI" that communicates with RPC manager 732): SPE **device** driver 736 (this SPE **device** driver is connected to an SPE 503 in the preferred embodiment); HPE Device Driver 738 (this HPE device driver is connected to an HPE 738... concurrently executing tasks may not be able to process using the same often-needed data structure in a single-threaded SPE 503. This may effectively **limit** the **number** of concurrent tasks to one. Additionally, single-threadedness may eliminate the capability of producing accurate summary budgets based on a number of concurrent tasks since... ...as the pages are compared and swapped. Even though this virtual paging solution might be workable for allowing single threading in some applications, the vendor **limitations** mentioned above may limit the use of such single threaded implementations in some cases to dedicated hardware. Any implementation that supports multiple users (e.g., "smart home" set tops, many desk tops and certain PDA applications, etc.) may hit **limitations** of a single threaded device in certain circumstances.

It is preferable when these **limitations** are unacceptable to **use** a full "multi-threaded" data structure write capabilities. For example, a type of "two-phase commit" processing of the type used by database vendors may... ...e.g., RTC 528).

Memory manager 578 is responsible for allocating and deallocating memory; supervising sharing of memory resources between processes; and enforcing memory access/**use restriction**. The SPE kernel/dispatcher memory manager 578 typically initially allocates all memory to kernel 552, and may be configured to permit only process-level access... ...may be represented using a bit map allocation vector, for example. In a memory block, a group of contiguous memory pages may start at a **specific** page **number**. The size of the block is measured by the number of memory pages it spans. Memory allocation may be recorded by setting/clearing the appropriate... ...storage 562. This request may be in the form of an RPC call to secure database manager 566 to retrieve the load module and associated **data** structures, and a call to encrypt/**decrypt** manager 556 to **decrypt** the load module before storing it in memory allocated by memory manager 578.

In somewhat more detail, the preferred embodiment executes a load module 1100... ...store the load module 1100. The load module execution manager 568 may copy the load module into that memory page, and queue the page for **decryption** and security checks by encrypt/**decrypt** manager 556 and **key** and tag manager 558. Once the page is **decrypted** and checked, the load module execution manager 568 checks the validation tag and inserts the load module into the list of paged in modules and...registration table 460 records, user/object table 462 records, URT 464 records, and PERC 808 records. This "open channel" task may preferably place calls to **key** and tag manager 558 to **validate** and correlate the tags associated with these various records to ensure that they are authentic and match. The preferred embodiment process then may write appropriate...

Dialog eLink: Order File History
13/3K/2 (Item 2 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

02018194

Secure transaction management
Gesicherte Transaktionsverwaltung
Gestion de transactions securisees

Patent Assignee:

- **Intertrust Technologies Corp.**; (2434323)
  955 Stewart Drive; Sunnyvale, CA 94085; (US)
  (Applicant designated States: all)

Inventor:

- **Ginter, Karl L.**
  10404 43rd Avenue; Beltsville, MD 20705; (US)
- **Shear, Victor H.**
  5203 Battery Lane; Bethesda, MD 20814; (US)
- **Sibert, W. Olin**
  30 Ingleside Road; Lexington, MA 02173-2522; (US)
- **Spahn, Francis J.**
  2410 Edwards Avenue; El Cerrito, CA 94530; (US)
- **Van Wie, David M.**
  51430 Willamette Street; 6 Eugene, OR 97401; (US)

Legal Representative:

- **Beresford, Keith Denis Lewis (28273)**
  BERESFORD & Co. 16 High Holborn; London WC1V 6BX; (GB)

	Country	Number	Kind	Date	
Patent	EP	1621960	A2	20060201	(Basic)
	EP	1621960	A3	20070110	
Application	EP	2005076129		19970829	
Priorities	US	706206		19960830	

Designated States:
AT; BE; CH; DE; DK; ES; FI; FR; GB; GR;
IE; IT; LI; LU; MC; NL; PT; SE;

Related Parent Numbers: Patent (Application):EP 922248 (EP 97939670)

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G06F-0021/00	A	I	F	B	20060101	20060913	H	EP

Abstract Word Count: 51
NOTE: 70
NOTE: Figure number on first page: 70

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS A	(English)	200605	249
SPEC A	(English)	200605	180527
Total Word Count (Document A) 180807			
Total Word Count (Document B) 0			
Total Word Count (All Documents) 180807			

Specification: ...a secure, flexible, general purpose foundation that can accommodate many different rights applications, that is, many different business models and their respective participant requirements.

A **rights** application under VDE is made up of special purpose pieces, each of which can correspond to one or more basic electronic processes needed for a...evolving agreement may develop between all value chain participants as content control information passes along its chain of handling. This evolving agreement can establish the **rights** of all parties to content usage information, including, for example, the nature of information to be received by each party and the pathway of handling... ...the present invention is the core secure transaction control arrangement, herein called an SPU (or SPUs), that typically must be present in each user's **computer**, other electronic appliance, or network. SPUs provide a trusted environment for generating **decryption keys**, encrypting and decrypting information, managing the secure communication of keys and other information between electronic appliances (i.e. between VDE installations and/or between plural...the request, or how the service request will be fulfilled. This feature supports families of services that may be scaled and/or customized for specific **applications**. Service requests can be forwarded and serviced by different processors and/or different sites as easily as they can be forwarded and serviced by a...concurrently executing tasks may not be able to process using the same often-needed data structure in a single-threaded SPE 503. This may effectively **limit** the **number** of concurrent tasks to one. Additionally, single-threadedness may eliminate the capability of producing accurate summary budgets based on a number of concurrent tasks since... ...tops, many desk tops and certain PDA applications, etc.) may hit limitations of a single threaded device in certain circumstances.

It is preferable when these **limitations** are unacceptable to **use** a full "multi-threaded" data structure write capabilities. For example, a type of "two-phase commit" processing of the type used by database vendors may... ...e.g., RTC 528).

Memory manager 578 is responsible for allocating and deallocating memory; supervising sharing of memory resources between processes: and enforcing memory access/**use restriction**. The SPE kernel/dispatcher memory manager 578 typically initially allocates all memory to kernel 552, and may be configured to permit only process-level access... ...may be represented using a bit map allocation vector. for example. In a memory block, a group of contiguous memory pages may start at a **specific** page **number**. The size of the block is measured by the number of memory pages it spans. Memory allocation may be recorded by setting/clearing the appropriate...SPU 500 is not being paused or probed, and other internal checks on the operation of SPU 500 are made to detect tampering.

The encryption/**decryption** engine 522 generates an interrupt when a **block** of **data** has been processed. The kernel interrupt handler 584 adjusts the processing status of the **block** -being encrypted or **decrypted**, and passes the **block** to the next stage of processing. The next block scheduled for the encryption service then has its key moved into the encrypt/decrypt engine 522...

Dialog eLink: Order File History
13/3K/6 (Item 6 from file: 348)
DIALOG(R)File 348: EUROPEAN PATENTS

01815760

Optical disk, method of manufacturing an optical disk and a reproduction apparatus
Optische Platte, Verfahren zur Herstellung einer optischen Platte und Wiedergabegerat
Disque optique, methode de fabrication d'un disque optique et methode de reproduction

Patent Assignee:

- **MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD**; (216883)
  1006, Oaza-Kadoma; Kadoma-shi, Osaka 571-8501; (JP)
  (Proprietor designated states: all)

Inventor:

- **Mitsuaki, Oshima**
  115-3, Minamitatsumi-choKatsuraNishikyo-ku; Kyoto-shiKyoto 615; (JP)
- **Yoshiho, Gotoh**
  5-1-3 Higashinakahama, Jyoto-ku,; Osaka-shiOsaka 536-0023; (JP)

Legal Representative:

- **Grunecker, Kinkeldey, Stockmair & Schwanhausser Anwaltssozietat (100721)**
  Maximilianstrasse 58; 80538 Munchen; (DE)

	Country	Number	Kind	Date	
Patent	EP	1480204	A1	20041124	(Basic)
	EP	1480204	B1	20070926	
Application	EP	2004020082		19951116	
Priorities	JP	94283415		19941117	
	JP	9516153		19950202	
	JP	95261247		19951009	

Designated States:
DE; FR; GB;

Related Parent Numbers: Patent (Application):EP 1120777 (EP 2001108949)

Related Divisions: Patent (Application):EP 1764782 (EP 2006027091)

International Patent Class (V7): G11B-007/00; G11B-020/10; G11B-023/30; G11B-013/04; G11B-019/06; G11B-007/09; G11B-020/00; G06F-001/00; G11B-019/12; G11B-007/24; G11B-007/26

International Classification (Version 8) IPC	Level	Value	Position	Status	Version	Action	Source	Office
G11B-0007/00	A	I	F	B	20060101	20040930	H	EP
G11B-0020/10	A	I	L	B	20060101	20040930	H	EP
G11B-0023/30	A	I	L	B	20060101	20040930	H	EP
G11B-0013/04	A	I	L	B	20060101	20040930	H	EP
G11B-0019/06	A	I	L	B	20060101	20040930	H	EP
G11B-0007/09	A	I	L	B	20060101	20040930	H	EP
G11B-0020/00	A	I	L	B	20060101	20040930	H	EP
G06F-0001/00	A	I	L	B	20060101	20040930	H	EP
G11B-0019/12	A	I	L	B	20060101	20040930	H	EP
G11B-0007/24	A	I	L	B	20060101	20040930	H	EP
G11B-0007/26	A	I	L	B	20060101	20040930	H	EP

Abstract Word Count: 78
NOTE: 1
NOTE: Figure number on first page: 1

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability	Available Text	Language	Update	Word Count
CLAIMS A		(English)	200448	251
SPEC A		(English)	200448	21512
CLAIMS B		(English)	200739	297

Fulltext Availability Available Text	Language	Update	Word Count
CLAIMS B	(German)	200739	286
CLAIMS B	(French)	200739	334
SPEC B	(English)	200739	21116
Total Word Count (Document A) 21766			
Total Word Count (Document B) 22033			
Total Word Count (All Documents) 43799			

Specification: ...be kept in the safe custody of the software maker. This greatly increases the security of encryption. (2) (A) Encryption (digital signature) of marking position **information**, etc. and **decryption** and reproduction of optical disk position **information**, etc., which have been briefly described in (1), will now be described in more detail. (B) Various mechanism for piracy prevention will also be described... ...measured at the optical disk maker, step 695 where the position information is encrypted (or a digital signature is appended), step 698 where the position **information** is **decrypted** (or the signature is verified or authenticated) in the reproduction apparatus, and step 735w where a check is made to determine whether the disk is... ...then compressed in step 735d, and the compressed position information H is obtained in step 735e. In step 695, the ciphertext of the compressed position **information** H is constructed. First, in step 695, a secret **key**, d, of 512 or 1024 bits, and secret keys, p and q, of 256 or 512 bits, are set, and in step 695b, encryption is... ...actually located in the position on the optical disk indicated by the position information. In step 736d, it is checked whether the difference between the **decrypted** position **information** and the actually measured position **information** falls within a tolerance. If the check is OK in step 736e, the process proceeds to step 736h to output software or data or execute... ...process from step 735a to step 735e is the same was that for the RSA function. In step 735f, authentication ciphertext for the compressed position **information** H is constructed. First, in step 735g, secret **keys** X (128 bits or over) and K are set, and in step 735h, a public system parameter G, a point on an ellipse, is determined ... ...reduce the time before the reproduction starts. This system therefore is suitable for application to consumer reproduction apparatus **(b)** Complex encryption (digital signature) using master **key**, subkey, etc. Not only the marking position **information** but **information** concerning the features of.contents of the software stored on the optical disk and an anti-piracy **identifier** are subjected to encryption (**digital** signature). Furthermore, two kinds of encryption keys, master key and subkey, are used. A specific example is described below in which a secret key encryption... ...software maker 9002, to be described later, via a communication line 9003. When a request for encryption is made from the software maker 9002, the **key** management center 9001 receives **data**, to be encrypted, via a network 9003 and encrypts the **data** using the master secret **key**. For simplicity of explanation, it is assumed here that the software maker 9002 also includes a disk manufacturing factory. Therefore, the software maker 9002 here... ...manufacturing process at the disk manufacturing factory illustrated in Figure 1, in addition to the production of software. That is, when manufacturing optical disks of **movie** software, **encryption** for prevention of illegal duplications is also performed. To accomplish the encryption, the software maker 9002 obtains an exclusive sub secret key from the key... ...performed using a sub public key corresponding to the sub secret key to be used in the second encryption step, and using a software feature **information** and anti-piracy identifier. The **information** is transferred to the **key** management center 9001 via the communication line 9003. The software feature information refers to the information describing the contents of the movie software written on... ...piracy prevention using second ciphertext is "1"; otherwise, the identifier is "0". In this example, the identifier is "1", needless to say. (1-2) The **key** management center 9001 encrypts the **information** transferred from the software maker 9002, by using the master secret **key** maintained at the center, and sends the encrypted **information** back to the software maker 9002. The thus created ciphertext is referred to as the first ciphertext. (1-3) The software maker 9002 records the... ...form a marking on each optical disk. (1-6) Further, the software maker 9002 detects the position of the marking and encrypts the obtained position **information** by using the sub secret **key** maintained at the maker. The thus encrypted **information** is referred to as the second ciphertext. Since it is created by encrypting the position information, the second ciphertext is different from one optical disk... ...the optical disk, and using the master public key stored in the ROM, decrypts the first ciphertext which contains in encrypted form the sub public **key** corresponding to the sub secret **key**, the software feature **information**, and the anti-piracy identifier (2-2) In the meantime, the player 9004 extracted the software feature information from the contents of the movie software recorded on the optical disk. The extracted software feature **information** is compared with the software feature **information** obtained by **decryption** in (2-1); if they do not agree, the optical disk is judged as being an illegally duplicated one, and the subsequent reproduction operation is... ...to make an illegal copy by altering the identifier to "0", his effort will be thwarted because the identifier is encrypted using the master secret' **key** after being combined with the software feature **information**, etc., as earlier described. (2-4) First, the second ciphertext recorded on the optical disk is read out. Then, the second ciphertext, which is the encrypted version of the position **information**, is **decrypted** using the sub public **key** obtained by

decryption in (2-1). (2-5) Using the **decrypted** position **information**, it is checked whether the marking is actually formed in the position on the optical disk indicated by the position information. Then, the actually measured marking position **information** is compared with the position **information decrypted** in (2-4). If they do not agree, the optical disk is judged as being an illegally duplicated one, and the reproduction operation is stopped... ...a Galois field, etc., and a one-direction hash function 864a such as SHA and MD5, to create software feature information 863. The software feature **information** 863 is then combined with a sub public **key** 861 special to the software maker and an anti-piracy identifier 865 as a copyright identifier, into one data block which is then encrypted in... ...and a flag of one bit to indicate whether software dubbing is prevented or not. Since the anti-piracy identifier 865 and the sub public **key** 861 are combined with the software feature **information** 863 unique to the software and are encrypted together by using the master secret key for public key encryption, it is not possible to alter them. The anti-piracy identifier 865 and the sub public **key** 861 are combined with the software feature **information** unique to the software, into one **data block** which is then encrypted by the secret **key**. If the software feature **information** 863 consists of 256 bits, there are 2256 possible variations. This means that when software feature information is extracted from data obtained by authoring a... ...not is therefore important. In the present invention, the anti-piracy identifier 865, including the anti-piracy identifier, is encrypted together with the software feature **information** by using a secret **key**, and recorded in a ciphertext recording section on the master disk. The reproduction apparatus decrypts the ciphertext with a prescribed public **key**.. This prevents illegal alterations from being made to either **data**. The only way left to pirates is to replace the whole portion of the first ciphertext, which contains the software feature information 863 and the... ...the latter as the second software feature information. Both kinds of information are the same in that they relate to the contents of the same **movie** software, but different in that the former is written in **encrypted** form at the time the optical disk is manufactured, while the latter is extracted by examining the contents of the actually recorded movie software at... ...with which the company maintains the security of its software on its own responsibility. As already described with reference to Figure 32, the software feature **information** and the sub public **key** the software company keeps are jointly encrypted, using the master secret key, into the first ciphertext. The reproduction apparatus decrypts the first ciphertext by applying... ...key on software locked or unlocked at their option. This in turn means that pirates cannot produce pirated disks unless they steal the sub secret **key information** unique to the software from the software maker. In Figure 32, the software maker combines disk physical position information 868 and disk ID 869, and... ...In Figure 36, the software company 871a first sets its own sub secret key 876, and computes the sub public key 861. The sub public **key** 861 is combined with the software feature **information** 861 of the software to be recorded, and transmitted to the key issuing center 872 via a network such as the Internet. The **key** issuing center 872 encrypts the combined **signal** with the master secret **key** 866a and sends back the encrypted master public key 858 to the software company. The software company combines it with the software, andsends the combined... ...the disk 800 is produced. Referring next to Figure 37, the software company 871b forms a marking on the disk 800, reads the marking position **information**, encrypts the position **information** with the sub secret **key** 876 corresponding to the sub public **key**, and, using a pulsed laser 813, records the encrypted **information** on the disk 800b in the form of a barcode. A detailed description of the recording operation has already be given and will not be... ...reproduction apparatus in step 876c, the first ciphertext is decrypted into plaintext in step 876b. In step 876d, the plaintext of the first software feature **information** 863 and sub public **key** 861 is obtained and in step 876f, it is checked against the second software feature information extracted using the one-direction hash function. If the... ...is stopped; if the check is OK, the sub public key is output in step 876h. If alterations have been made to the sub public **key** or software attributes by a pirate, the two kinds of **information** do not agree, so that the reproduction of an illegal disk is prevented. The legitimate sub **public key** is thus obtained at the reproduction **apparatus**. In the disk **check** step 875, the sub **public key** is input in step 876k, and the second ciphertext, i.e., the public key cipher 859 (see Figure 32), is reproduce in step 876m. In step 876n, the second ciphertext is decrypted into plaintext by using the sub public **key**, and in step 876p, the marking position **information** is obtained. In this case, the marking position **information** cannot be altered illegally unless the sub secret **key** 876 (see Figure 32) corresponding to the sub public key is leaked out. In step 876p, the actual position of the marking formed on the...first feature of the encryption system of the present invention is the use of two encryption functions, a public key encryption function and a secret **key** encryption function, when encrypting marking position **information**, etc. on each optical disk. The following description deals with problems encountered when actually implementing a piracy prevention method that uses public key cipher, and also deals with a method of implementation. The public **key** cipher here refers to the position **information** encrypted using a public **key** encryption function (for example, an RSA function). From the security point of view, it is desirable that all reproduction apparatus be equipped with a public... ...few minutes to process the public key. This means that the user has to wait a few minutes before an image is reproduced from a **DVD**. This poses a problem in employing the public key **cipher** system in consumer product. Since, at the present level, public key cipher cannot be processed by the CPU used in consumer products, for the present... ...for consumer reproduction apparatus because it requires a small amount of processing time. However, in the case of secret key cipher, since the secret encryption **key** can be easily **deciphered** from cipher **decoder information**, the secret **key** cipher will lose its anti-piracy effect once deciphered. Therefore, transferring to public key cipher which is difficult to decipher is imperative in the future... ...later with reference to Figure 29. First, when

reproducing the optical disk of Figure 39 on a first-generation reproduction apparatus equipped with a secret **key** cipher **decoder** 881, the first physical feature **information** (corresponding to the encrypted version of the position **information**) unique to the legitimate disk is read from the secret **key** cipher recording portion 879 on the disk, and decrypted by the secret **key** cipher **decoder** 881 into plaintext. Further, the second physical feature **information** (corresponding to the measured position information) of the disk is measured, and the two kinds of physical **information** are compared. In the case of a... ...pirate, as earlier described, the pirate can produce illegal disks in large quantities by illegally creating the secret key cipher. In that case, since the **secret key** decoder 881 in the first-generation reproduction **apparatus checks** only the **secret key** cipher, the comparison **checks** OK as shown in step 878d, allowing the illegal pirated disk to be reproduced. However, by that time in the future, second-generation reproduction apparatus... ...on the second-generation reproduction apparatus, as shown in step 878b. On the other hand, when a pirated disk is inserted for reproduction, the reproduction **apparatus checks** only the **public key** cipher, as shown in step 878e, whether the secret key cipher is deciphered or not. As a result, the anti-piracy function of the public... ...piracy prevention method at the master disk level that uses the physical feature information of the master disk as shown in Figure 13. The above-**illustrated** example has the feature that, when performing **encryption**, the same **information** is encrypted by using a public **key** encryption function and a secret **key** encryption function separately, and the respectively encrypted versions of the **information** are recorded on the disk. Accordingly, when a transition is made in future from the current player equipped with a decoder, based on an 8... ...can be used effectively on either type of player. (B) Other mechanisms will be described. (a) We will describe another specific example of the public **key**/secret **key** combination type in which the software feature **information**, ID number, and marking position information.are encrypted (see Figure 29). The ID number refers to the number assigned to each disk for identifying the... ...sub secret key, while in the present example, encryption is performed only with master secret key without using a key corresponding to the sub secret **key**. More specifically, as shown in Figure 29, the above combined **signal** is encoded in a secret **key** encryption section 832 by using a secret **key** 834 for secret **key** encryption. The same combined **signal** is also encoded in a public **key** encryption section 831 by using a secret key 833 for public key encryption. In this way, public key cipher is used in conjunction with secret... ...546 has already been described with reference to Figure 14, and therefore, explanation will not be repeated here. In the encryption section 830, the combined **signal** of the physical feature **information** is encoded in the public **key** encryption section 831, such as RSA, by using the secret key 833 for public key encryption. The above public key cipher and the secret key... ...to provide error correction of errors in the barcode recorded data of the invention against a disk scratch that may be caused in the worst **condition** in consumer **use**. The principle of the pulse width modulation method will be described with reference to the same figure. This-method eliminates the need for the first ciphertext by the master secret key and the second ciphertext by the sub secret **key**. In this method, the software feature **information**, the position **information**, and the ID number are combined together for encryption. Billions of ROM disks are produced annually. Therefore, there is a possibility that a disk that... ...tertiary-record by the HMST method. As shown in Figure 35, in process (2), the software maker may produce a disk 844b on which the **ID number unique** to the disk and a private key used for secret communication with a user are recorded. The disk 844c, 844d can be reproduced without requiring... ...video signal or the like is recorded on a disk 844e. A brief operational description of MPEG scrambling will be given below. An MPEG compressed **video** signal is split between a variable-length **encoder** for AC components and a fixed-length encoder, each containing a random number adder, for scrambling. In the present invention, a descrambling signal is encrypted by an encryption encoder using a one-direction function. Further, a portion of a compression program in an **image** compression controller is compressed by the **encryption encoder**. This makes it difficult for a replicating company to exchange the encryption encoder with an illegal one. Accordingly, only legitimate disks are decrypted with sub... ...That is, in process (4) of Figure 35, using a master secret key the software company encrypts the disk ID number and a sub public **key** for **decoding** the descrambling **signal**, and secondary-records the encrypted text by barcode on the disk, thus completing the disk 844f. Since the disk 844f are scrambled, the disk cannot...

00935970

A SYSTEM AND METHOD FOR LOADING APPLICATIONS ONTO A SMART CARD
SYSTEM UND VERFAHREN ZUM LADEN VON MEHRFACHEN ANWENDUNGEN IN EINE CHIPKARTE
SYSTEME ET PROCEDE POUR CHARGER DES APPLICATIONS DANS UNE CARTE A PUCE

Patent Assignee:

- **GEMPLUS**; (1027408)
  Avenue du Pic de Bertagne, Parc d'Activites de Gemenos, BP 100; 13881 Gemenos Cedex; (FR)
  (Proprietor designated states: all)

Inventor:

- **LISIMAQUE, Gilles**
  Gemplus S.C.A., Z.I. Athelia III, Voie Antiope; F-13705 La Ciotat; (FR)
- **PEYRET, Patrice**
  Gemplus S.C.A., Z.I. Athelia III, Voie Antiope; F-13705 La Ciotat; (FR)

	Country	Number	Kind	Date	
Patent	EP	858644	A1	19980819	(Basic)
	EP	858644	B1	20030326	
	WO	98009257		19980305	
Application	EP	97937756		19970829	
	WO	97IB1042		19970829	
Priorities	US	706396		19960830	

Designated States:
AT; BE; CH; DE; DK; ES; FI; FR; GB; GR;
IE; IT; LI; LU; MC; NL; PT; SE;

International Patent Class (V7): G07F-007/10
NOTE: No A-document published by EPO

Legal Status Type	Pub. Date	Kind	Text

Language Publication: English
Procedural: English
Application: English

Fulltext Availability	Available Text	Language	Update	Word Count
CLAIMS B		(English)	200313	689
CLAIMS B		(German)	200313	670
CLAIMS B		(French)	200313	796
SPEC B		(English)	200313	5722
Total Word Count (Document A) 0				

Fulltext Availability Available Text	Language	Update	Word Count
Total Word Count (Document B) 7877			
Total Word Count (All Documents) 7877			

Specification: ...making any change in the use rights of an application stored in the smart card, and may prevent unwanted or illegal attempts to decrease the **use rights** of an **application**. This authentication and **validation** may be conducted using cryptographic systems, such as **public key** encryption, or any other

IV. Text Search Results from Dialog

A. NPL Files, Abstract

```
File  35:Dissertation Abs Online 1861-2009/Jun
        (c) 2009 ProQuest Info&Learning
File 474:New York Times Abs 1969-2009/Jul 13
        (c) 2009 The New York Times
File 475:Wall Street Journal Abs 1973-2009/Jul 13
        (c) 2009 The New York Times
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
        (c) 2002 Gale/Cengage
File  65:Inside Conferences 1993-2009/Jul 13
        (c) 2009 BLDSC all rts. reserv.
File  99:Wilson Appl. Sci & Tech Abs 1983-2009/Jun
        (c) 2009 The HW Wilson Co.
File   2:INSPEC 1898-2009/Jul W1
        (c) 2009 The IET
File 256:TecTrends 1982-2009/Jul
        (c)2009 Info.Sources Inc.All rights reserved


Set     Items   Description
S1        840   (CONFIRM??? OR CONFIRMATION OR ACKNOWLEDG??? OR ACKNOWLEDGEMENT OR
AFFIRM??? OR ATTEST??? OR CERTIFY??? OR CHECK??? OR SUBSTANTIAT??? OR VERIFY??? OR
PROVE? ? OR PROVING OR VALIDAT??? OR VALIDITY OR AUTHENTICITY) (10N) ((PUBLIC OR
PRIVATE OR SYSTEM OR SECRET OR SYMMETRIC OR SYNCHRONOUS OR CONTENT OR ASSESS OR
DECRYPTION OR ASYMMETRIC OR SYMMETRIC)()KEY? ? OR PKI OR PGP OR WEB()TRUST)

S2         48   S1 (5N) (PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR
DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR
DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR
WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?)

S3      83224   (USAGE OR USE) (3N) (CONDITION? ? OR TERMS OR RULE? ? OR
RESTRICTION? ? OR RIGHTS OR LIMITATION? ?) OR (LIMIT??? OR RESTRICT??? OR SPECIFI??
OR PERMITTED OR FIXED OR DEFINED OR STIPULATED OR PREDEFINED OR PRESET OR
PREESTABLISHED OR PREDETERMINED) (3N) (NUMBER OR TIMES OR COPIED OR COPIES OR
PLAYED OR DOWNLOAD??) OR AVAILABILITY()DATES OR USAGE()PERIODS

S4      28165   (CRYPTOGRA? OR (ELECTRONIC OR DIGITAL)()(SEAL? ? OR SIGNATURE? ? OR
CERTIFICAT??? OR ENVELOPE? ?) OR ENCRYPT??? OR CIPHER? ? OR CYPHER? ? OR HASH?? OR
ENCOD??? OR ENC?PHER??) (10N) (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR
ART OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR
PHOTOGRAPH OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS
OR ALBUM OR ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S5      73946   (UNENCOD??? OR UNCOD??? OR UNENCRYPT??? OR DECRYPT??? OR DECOD???
OR DEC?PHER??? OR KEY OR KEYS) (10N) (MESSAGE? ? OR SIGNAL? ? OR PACKET? ? OR
TRANSMISSION? ? OR BLOCK? ? OR INFORMATION OR DATA)
```

```
S6       72923   (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR
ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR
PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR AUDIOVISUAL OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR PRODUCT OR UNIQUE OR
SECURITY OR DIGITAL) (5N) (ID OR IDS OR IDENTIFICATION OR NUMBER? ? OR IDENTIFIER?
?)

S7           1   AU=(MAARI, K? OR MAARI K? OR MAARI (1N) (K OR KOICHI))
S8           0   S2 AND S3
S9          21   S2 AND (S3 OR S4 OR S5 OR S6)
S10          6   S9 NOT PY>1997
S11          6   RD  (unique items)
S12         11   S1 AND S3
S13         11   S12 NOT S11
S14          1   S13 NOT PY>1997
S15        239   S3 AND S4
S16         31   S15 AND S5
S17          2   S16 AND S6
S18         42   S2 NOT (S11 OR S14 OR S17)
S19          7   S18 NOT PY>1997
S20          7   RD  (unique items)
S21          0   S7 AND (S1 OR S2 OR S3 OR S4 OR S5 OR S6)
```

Dialog eLink: USPTO Full Text Retrieval Options

11/5/1 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC

06792777
Title: Another countermeasure to forgeries over message recovery signature
Author(s): Miyaji, A.
Author Affiliation: Matsushita Electr. Ind. Co. Ltd., Kadoma , Japan
Journal: IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences , vol.E80-A , no.11 , pp.2192-200
Publisher: Inst. Electron. Inf. & Commun. Eng
Country of Publication: Japan
Publication Date: Nov. 1997
ISSN: 0916-8508
SICI: 0916-8508(199711)E80A:11L.2192:ACFO;1-Q
CODEN: IFESEX
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: Nyberg and Rueppel (1993) recently proposed a new ElGamal-type digital signature scheme with message recovery feature and its six variants. The advantage of small signed **message** length is effective especially in some **applications** like **public key certifying** protocols or the key exchange. But two forgeries that present a real threat over such **applications** are pointed out. In **certifying public keys** or key exchanges, redundancy is not preferable in order to store or transfer small data. Therefore the current systems should be modified in order to integrate the Nyberg-Rueppel's signature into such applications. However, there has not been such a research that prevents the forgeries directly by improving the signature scheme. In this paper, we investigate a condition to avoid the forgeries directly. We also show some new message recovery signatures strong against the forgeries by adding a negligible computation amount to their signatures, while not

increasing the signature size. The new scheme can be integrated into the above application without modifying the current systems, while maintaining the security (*16 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: protocols; public key cryptography
Identifiers: forgery countermeasure; message recovery signature; ElGamal-type digital signature scheme; small signed **message** length; **public key** certifying protocols; **key** exchange; **data** security
Classification Codes: B6120B (Codes); B6150M (Protocols); C6130S (Data security); C5640 (Protocols)
INSPEC Update Issue: 1998-001

11/5/2 (Item 2 from file: 2)
DIALOG(R)File 2: INSPEC

06039183
Title: A **digital signature scheme based on linear error-correcting block codes**
Author(s): Alabbadi, M.; Wicker, S.B.
Author Affiliation: KACST, Riyadh, Saudi Arabia
Book Title: Advances in Cryptology - ASIACRYPT'94. 4th International Conference on the Theory and Applications of Cryptology. Proceedings
Inclusive Page Numbers: 238-48
Publisher: Springer-Verlag, Berlin
Country of Publication: Germany
Publication Date: 1995
Conference Title: Advances in Cryptology - ASIACRYPT '94. 4th International Conference on the Theory and Applications of Cryptology
Conference Date: 28 Nov.-1 Dec. 1994
Conference Location: Wollongong, NSW, Australia
Conference Sponsor: Univ. Wollongong
Editor(s): Pieprzyk, J.; Safavi-Naini, R.
ISBN: 3 540 59339 X
Number of Pages: xii+430
Language: English
Document Type: Conference Paper (PA)
Treatment: Theoretical or Mathematical (T)
Abstract: A true trapdoor digital signature scheme is presented. The scheme uses linear error-correcting block codes in a manner similar to that of the McEliece public-key cryptosystem, the Rao-Nam private-key cryptosystem, and the three digital signature schemes proposed by Xinmei (1990), Harn and Wang (1992), and the authors. All these digital signature schemes have been shown to be susceptible to a number of attacks. The signature scheme described in this paper derives its security from the complexity of three problems: the **decoding** of general linear error-correcting **block** codes, the factoring of large matrices, and the derivation of a matrix from its right inverse. It is shown that the proposed scheme is resistant to the attacks that proved successful when used against the aforementioned digital signature schemes as well as other attacks. The required public key storage is about $3n^2$ bits. The complexity of the signature generation and validation algorithms are $O(n^2)$ and $O(nk)$ bit operations respectively, thus making the scheme amenable to use in high data rate applications (*14 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: block codes; computational complexity; **data** communication; error correction codes; linear codes; matrix inversion; **public key** cryptography
Identifiers: digital signature scheme; linear error-correcting **block** codes; trapdoor digital signature scheme; **public key** storage; signature generation complexity; **validation** algorithms; **high data** rate **applications**; matrix derivation
Classification Codes: B6120B (Codes); B0210 (Algebra); C6130S (Data security); C1110 (Algebra); C4240C (Computational complexity)
INSPEC Update Issue: 1995-034

Copyright: 1995, IEE

Dialog eLink: USPTO Full Text Retrieval Options
11/5/3 (Item 3 from file: 2)
DIALOG(R)File 2: INSPEC

05726851
Title: Private-key encryption based on concatenation of codes
Author(s): Al Jabri, A.Kh.; Al-Thukair, F.; Mirza, A.
Author Affiliation: Dept. of Electr. Eng., King Saud Univ., Riyadh, Saudi Arabia
Journal: IEE Proceedings-Communications , vol.141 , no.3 , pp.105-10
Country of Publication: UK
Publication Date: June 1994
ISSN: 1350-2425
CODEN: IPCOED
U.S. Copyright Clearance Center Code: 1350-2425/94/$7.50+0.00
Item Identifier (DOI): 10.1049/ip-com:19941137
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: Public-key algebraic encryption (PUAE) has certain advantages that make it attractive in some **applications**. Variants of PUAE for **private-key** algebraic encryption (PRAE); have been proposed subsequently. PRAE is **proven** to be insecure under chosen plaintext attack. In the paper, some invariants of PRAE are studied, and a private-key cryptosystem based on concatenation of codes is proposed and analysed. The new system is, composed of short-length codes and is designed to avoid the weaknesses in other PRAE systems. The system looks secure against known attacks. Some methods to improve the system information rate and security are also suggested (*11 refs.*)
Subfile(s): B (Electrical & Electronic Engineering)
Descriptors: codes; public key cryptography
Identifiers: private-key encryption; public-key algebraic encryption; plaintext attack; private-**key** cryptosystem; codes concatenation; short-length codes; system **information** rate; system security
Classification Codes: B6120B (Codes)
INSPEC Update Issue: 1994-030
Copyright: 1994, IEE

Dialog eLink: USPTO Full Text Retrieval Options
11/5/4 (Item 4 from file: 2)
DIALOG(R)File 2: INSPEC

05500189
Title: Immunizing public key cryptosystems against chosen ciphertext attacks
Author(s): Zheng, Y.; Seberry, J.
Author Affiliation: Dept. of Comput. Sci., Wollongong Univ., NSW, Australia
Journal: IEEE Journal on Selected Areas in Communications , vol.11 , no.5 , pp.715-24
Country of Publication: USA
Publication Date: June 1993
ISSN: 0733-8716
CODEN: ISACEM
U.S. Copyright Clearance Center Code: 0733-8716/93/$03.00

Item Identifier (DOI): 10.1109/49.223871
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: Three methods for strengthening public key cryptosystems in such a way that they become secure against adaptively chosen ciphertext attacks are presented. In an adaptively chosen ciphertext attack, an attacker can query the deciphering algorithm with any ciphertext except for the exact object ciphertext to be cryptanalyzed. The first strengthening method is based on the use of one-way hash functions, the second on the use of universal hash functions, and the third on the use of **digital signature** schemes. Each method is **illustrated** by an example of a public key cryptosystem based on the intractability of computing discrete logarithms in finite fields. Security of the three example cryptosystems is formally **proved**. Two other issues, namely, applications of the methods to **public key** cryptosystems based on other intractable problems and enhancement of **information** authentication capability to the cryptosystems, are also discussed (*28 refs.*)
Subfile(s): B (Electrical & Electronic Engineering)
Descriptors: **message** authentication; public **key** cryptography
Identifiers: immunization methods; public key cryptosystems; ciphertext attacks; deciphering algorithm; strengthening method; one-way hash functions; universal hash functions; digital signature; discrete logarithms; information authentication
Classification Codes: B6120B (Codes)
INSPEC Update Issue: 1993-040

11/5/6 (Item 6 from file: 2)
DIALOG(R)File 2: INSPEC

04287318
Title: A stitch in crime.... smart card security solutions
Author(s): Fifield, K.J.; Gordon, J.
Author Affiliation: Fraser Williams, London, UK
Inclusive Page Numbers: 10 pp.
Publisher: PLF Commun, Peterborough
Country of Publication: UK
Publication Date: 1988
Conference Title: SMART CARD '88: International Conference and Workshop on Smart Card Applications and Technologies
Conference Date: 20-22 June 1988
Conference Location: London, UK
Number of Pages: 3 vol. (222+174+44)
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Outlines the various areas of computer network vulnerability and the smart card techniques used to make the system secure. This includes personal authentication and data validation using private or public key schemes. A DES based system is described together with a review of the advantages and disadvantages. The weaknesses of such a private key system are highlighted and the more secure public key RSA system is explained. The disadvantages of implementation into a smart card are mentioned, and why the search for an implementable public key system is a high priority. Present development effort shows that the Fiat-Shamir technique can fit the bill. It is implementable for an 8-bit smart card processor and takes 5-10% of the time of the RSA algorithm. The technique is described and the mathematical reasons why it is faster, and as secure, as RSA pointed out. Application examples are given together with FW project experience to date. The resulting solution shows that smart cards can provide a very high level of computer system protection. Password hacking can be radically reduced by the Fiat-Shamir smart card solution together with line tapping, line diversion and unauthorised program modification. It can also prove that a user is who he says he is without knowing the process that generates the initial challenge. This is a substantial step forward in providing a means to legally resolve any dispute of authentication be it personal or data, with a smart card (*1 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)

Descriptors: computer crime; computer networks; cryptography; smart cards
Identifiers: password hacking; crime; smart card security solutions; computer network vulnerability; personal authentication; data validation; public key schemes; DES based system; private **key** system; Fiat-Shamir technique ; 8-bit smart card processor; RSA algorithm; FW project; computer system protection; line tapping; line diversion; unauthorised program modification
Classification Codes: B6120B (Codes); B6210L (Computer communications); C6130 (Data handling techniques); C0310D (Computer installation management); C5620 (Computer networks and techniques)
INSPEC Update Issue: 1989-003
Copyright: 1989, IEE

14/5/1 (Item 1 from file: 35)
DIALOG(R)File 35: Dissertation Abs Online

01608996 ORDER NO: NOT AVAILABLE FROM UNIVERSITY MICROFILMS INT'L.
ON THE SECURITY OF CRYPTOGRAPHIC ALGORITHMS (PSEUDORANDOM, SUPERPOLYNOMIAL)

Author: COLBERT, BERNARD
Degree: PH.D.
Year: 1997
Corporate Source/Institution: UNIVERSITY OF NEW SOUTH WALES (AUSTRALIA) (0423)
Source: Volume 5809B of Dissertations Abstracts International.
PAGE 4846 .
Descriptors: MATHEMATICS ; COMPUTER SCIENCE
Descriptor Codes: 0405; 0984

In this thesis we consider the provability of the security of cryptographic algorithms--that is, proving that a particular cryptographic algorithm is immune to cryptanalytic attacks. To this end, we formalise cryptanalytic attacks and the criteria for "breaking" the cryptographic algorithm. This formal model is used to show that if an algorithm exists that determines if an efficient attack against the cryptographic algorithm exists, then a feasible universal cryptanalytic attack exists. However, we demonstrate that a feasible universal cryptanalytic attack does not exist; and thus, conclude that there is no algorithm that determines the immunity of cryptographic algorithms to attacks.

Our consideration turns to other methods of demonstrating the security of cryptographic algorithms: we consider families of cryptographic algorithms indexed by block size: these are known as cryptosystems. Algorithms derived from pseudorandom cryptosystems have strong cryptographic properties, in particular, resilience against attack. We find some sufficient conditions for pseudorandom cryptosystems and conclude that they are infeasible. We then determine a necessary condition for pseudorandom cryptosystems: that the keyspaces $\{ K\sb{n}\}\sb{n\varepsilon\rm N}$ must grow as $\vert K\sb{n}\vert \ \geq\ \xi (n)2\sp{n}$ for a superpolynomial function ξ. We analyse **public-key** cryptosystems and conclude that **proving** pseudorandomness for feasible cryptosystem requires complexity assumptions.

We consider the design of cryptographic algorithms that are apparently strong but are vulnerable to a specific, secret attack. These algorithms are used as a model for an analysis to demonstrate that cryptographic design criteria are necessary but not sufficient **conditions**; we also **use** the model to determine how to secure the cryptographic algorithm against the secret attack.

17/5/2 (Item 2 from file: 2)
DIALOG(R)File 2: INSPEC

05776252
Title: Multiplexing of variable rate encoded streams
Author(s): Haskell, B.G.; Reibman, A.R.
Author Affiliation: AT&T Bell Labs., Holmdel, NJ, USA
Journal: IEEE Transactions on Circuits and Systems for Video Technology , vol.4 , no.4 , pp.417-24

Country of Publication: USA
Publication Date: Aug. 1994
ISSN: 1051-8215
CODEN: ITCTEM
U.S. Copyright Clearance Center Code: 1051-8215/94/$04.00
Item Identifier (DOI): 10.1109/76.313136
Language: English
Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Discusses the problem of multiplexing several variable rate encoded streams into a single stream. Moreover, in order to facilitate editing of the resulting stream it is required that data generated during the same time interval is multiplexed together. Particular emphasis is placed on controlling encoder rates and combining data in such a way as to avoid overflow and underflow of buffers at encoder and **decoder**. Applications include satellite or cable **transmission** of a **fixed number** of different **video** channels, multimedia presentations with multiple video streams, and video on demand (*6 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: codecs; decoding; demultiplexing; demultiplexing equipment; image coding; multimedia systems; multiplexing equipment; telecommunications control; video equipment; video signals
Identifiers: variable rate encoded streams; multiplexing; **encoder** rates; overflow; underflow; buffers; **encoder**; **decoder**; satellite **transmission**; cable **transmission**; **video** channels; multimedia; multiple **video** streams; video on demand
Classification Codes: B6230 (Switching centres and equipment); B6120B (Codes); B6140C (Optical information, image and video signal processing); B6430 (Television equipment, systems and applications); C5260B (Computer vision and image processing techniques); C3370P (Control applications in video and audio techniques)
INSPEC Update Issue: 1994-039

Dialog eLink:
20/5/1 (Item 1 from file: 99)
DIALOG(R)File 99: Wilson Appl. Sci & Tech Abs

1173534 **H.W. Wilson Record Number:** BAST94042141
Private-key encryption based on concatenation of codes

Al Jabri, A. Kh ; Al-Thukair, F; Mirza, A
IEE Proceedings. Communications v. 141 (June '94) p. 105-10
Document Type: Feature Article **ISSN:** 1350-2425 **Language:** English **Record Status:** New record

Abstract: Public-key algebraic encryption (PUAE) has certain advantages that make it attractive in some **applications**. Variants of PUAE for **private-key** algebraic encryption (PRAE) have been proposed subsequently. PRAE is **proven** to be insecure under chosen plaintext attack. In the paper, some invariants of PRAE are studied, and a private-key cryptosystem based on concatenation of codes is proposed and analysed. The new system is composed of short-length codes and is designed to avoid the weaknesses in other PRAE systems. The system looks secure against known attacks. Some methods to improve the system information rate and security are also suggested. Reprinted by permission of the publisher.

Descriptors: Public key cryptosystems; Concatenated codes; Information rates ;

20/5/2 (Item 1 from file: 2)
DIALOG(R)File 2: INSPEC

06781779
Title: Research directions for automated software verification: using trusted hardware
Author(s): Devanbu, P.; Stubblebine, S.

Author Affiliation: Inf. Syst. & Services Res. Center, AT&T Labs.-Res., Florham, NJ, USA
Book Title: Proceedings. 12th IEEE International Conference Automated Software Engineering (Cat. No.97TB100200)
Inclusive Page Numbers: 274-9
Publisher: IEEE Comput. Soc, Los Alamitos, CA
Country of Publication: USA
Publication Date: 1997
Conference Title: Proceedings 12th IEEE International Conference Automated Software Engineering
Conference Date: 1-5 Nov. 1997
Conference Location: Incline Village, NV, USA
Conference Sponsor: IEEE Comput. Soc. NASA Ames Res. Center AAAI ACM SIGART ACM SIGSOFT Microsoft
ISBN: 0 8186 7961 1
U.S. Copyright Clearance Center Code: 0 8186 7961 1/97/$10.00
Item Identifier (DOI): 10.1109/ASE.1997.632848
Number of Pages: xix+321
Language: English
Document Type: Conference Paper (PA)
Treatment: Practical (P)
Abstract: Service providers hosting software on servers at the request of content providers need assurance that the hosted software has no undesirable properties. This problem applies to browsers which host applets, networked software which can host software agents, etc. The hosted software's properties are currently verified by testing and/or verification processes by the hosting computer. This increases cost, causes delay, and leads to difficulties in version control. By furnishing content providers with a physically secure computing device with an embedded certified private key, such properties can be verified and/or enforced by the secure computing device at the content provider's site; the secure device can verify such properties, statically whenever possible, and by inserting checks into the executable binary when necessary. The resulting binary is attested by a trusted signature, and can be hosted with confidence. The position paper is a preliminary report that outlines scientific and engineering goals in this project (*15 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: computer networks; configuration management; program testing; program verification; security of data
Identifiers: automated software verification; trusted hardware; service providers; servers; content providers; hosted software; browsers; applets; networked software; software agents; testing; hosting computer; version control; physically secure computing **device**; embedded certified **private key**; **checks**; executable binary; trusted signature; scientific goals; engineering goals
Classification Codes: C6110F (Formal methods); C6150G (Diagnostic, testing, debugging and evaluating systems); C6115 (Programming support); C6130S (Data security); C6150N (Distributed systems software)
INSPEC Update Issue: 1997-049

20/5/3 (Item 2 from file: 2)
DIALOG(R)File 2: INSPEC

05923243
Title: The first experimental cryptanalysis of the Data Encryption Standard
Author(s): Matsui, M.
Author Affiliation: Lab. of Comput. & Inf. Syst., Mitsubishi Electr. Corp., Kanagawa, Japan
Book Title: Advances in Cryptology - CRYPTO '94. 14th Annual International Cryptology Conference. Proceedings
Inclusive Page Numbers: 1-11
Publisher: Springer-Verlag, Berlin
Country of Publication: Germany
Publication Date: 1994
Conference Title: Advances in Cryptology - CRYPTO '94. 14th International Cryptology Conference Proceedings
Conference Date: 21-25 Aug. 1994
Conference Location: Santa Barbara, CA, USA
Conference Sponsor: Int. Assoc. Cryptologic Res. IEEE Comput. Soc. Tech. Committe on Security & Privacy

Editor(s): Desmedt, Y.G.
ISBN: 3 540 58333 5
Number of Pages: vi+438
Language: English
Document Type: Conference Paper (PA)
Treatment: Experimental (X)
Abstract: Describes an improved version of linear cryptanalysis and its application to the first successful computer experiment in breaking the full 16-round DES. The scenario is a known-plaintext attack based on two new linear approximate equations, each of which provides candidates for 13 secret key bits with negligible memory. Moreover, reliability of the key candidates is taken into consideration, which increases the success rate. As a result, the full 16-round DES is breakable with a high probability of success if 2^{43} random plaintexts and their ciphertexts are available. The author carried out the first experimental attack using 12 **computers** to **confirm** this: he finally reached all of the 56 **secret key** bits in 50 days, out of which 40 were spent for generating plaintexts and their ciphertexts and only 10 days were spent for the actual key search (*7 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: cryptography; equations; mathematics computing; reliability; telecommunication computing
Identifiers: linear cryptanalysis; Data Encryption Standard; 16-round DES; known-plaintext attack; linear approximate equations; secret key bits; negligible memory; key candidate reliability; success rate; random plaintexts; ciphertexts; key search
Classification Codes: B6120B (Codes); C6130S (Data security); C7310 (Mathematics computing); C7410F (Communications computing)
INSPEC Update Issue: 1995-014

Dialog eLink:
20/5/4 (Item 3 from file: 2)
DIALOG(R)File 2: INSPEC

05329813
Title: Lyndon trees
Author(s): Subramanian, K.G.; Siromoney, R.; Mathew, L.
Author Affiliation: Dept. of Math., Madras Christian Coll., India
Journal: Theoretical Computer Science , vol.106 , no.2 , pp.373-83
Country of Publication: Netherlands
Publication Date: 14 Dec. 1992
ISSN: 0304-3975
CODEN: TCSCDI
U.S. Copyright Clearance Center Code: 0304-3975/92/$05.00
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: Lyndon trees are introduced as a generalization of Lyndon words, and the basic properties studied. A correspondence between the sets of Lyndon words and Lyndon trees is established. A unique factorization theorem for factoring a tree in terms of Lyndon trees is **proved**. As an **application** of this result, a **public key** cryptosystem for trees is constructed, for which encryption and decryption are easy but cryptanalysis is hard (*11 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: public key cryptography; trees (mathematics)
Identifiers: Lyndon trees; Lyndon words; factorization theorem; public key cryptosystem; encryption; decryption; cryptanalysis
Classification Codes: C6130S (Data security); C1160 (Combinatorial mathematics)
INSPEC Update Issue: 1993-003

Copyright: 1993, IEE

Dialog eLink: USPTO Full Text Retrieval Options
20/5/5 (Item 4 from file: 2)
DIALOG(R)File 2: INSPEC

04280402
Title: Cryptographic programs
Author(s): Ruhland, J.
Journal: Chip , no.9 , pp.94-8
Country of Publication: West Germany
Publication Date: Sept. 1988
ISSN: 0170-6632
CODEN: CHIPDP
Language: German
Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: The author loosely surveys the theory and practice of various modern cryptographic methods. He mentions such topics as RSA code, public key systems, time locked codes and error checks, and gives a short introductory description to the mProtect and Protect programs. He also names three cryptographic programs available to the public-i.e. PC Crypt, The Confidant and Encode/Decode-and four Pascal programs for performing given encrypting tasks (*0 refs.*)
Subfile(s): B (Electrical & Electronic Engineering); C (Computing & Control Engineering)
Descriptors: codes; cryptography; Pascal listings
Identifiers: cryptographic methods; RSA code; **public key** systems; time locked codes; error **checks**; mProtect; Protect **programs**; cryptographic **programs**; **PC** Crypt; The Confidant; Encode/Decode; Pascal programs; encrypting tasks
Classification Codes: B6120B (Codes); C6130 (Data handling techniques)
INSPEC Update Issue: 1989-003
Copyright: 1989, IEE

Dialog eLink: USPTO Full Text Retrieval Options
20/5/6 (Item 5 from file: 2)
DIALOG(R)File 2: INSPEC

03801927
Title: Group parity check system for important information
Author(s): Tanaka, H.; Momohara, T.; **Kaneku**, S.
Author Affiliation: Fac. of Eng., Kobe Univ., Japan
Journal: Electronics and Communications in Japan, Part 1 (Communications) , vol.68 , no.2 , **pp.**35-9
Country of Publication: USA
Publication Date: Feb. 1985
ISSN: 8756-6621
CODEN: ECJCED
U.S. Copyright Clearance Center Code: 8756-6621/85/0002-0035$7.50/0
Language: English
Document Type: Journal Paper (JP)
Treatment: Theoretical or Mathematical (T)
Abstract: Can we prevent human deception or computer crime by cryptography? The main functions of cryptography are `secrecy' and `authentification', and they are certainly effective for those outside a computer system. However, for the

professional insiders who want to attempt deception, no cryptosystem will work well even if the information is protected by advanced cryptography because of the dependence on human conscience. Therefore, based on the concept that only humans can check human deception, the authors propose a new scheme of data security, the 'group parity check system for important information'. This scheme checks human deception arising in information input by mutual surveillance among people related to the information system. Furthermore, they show how to realize this scheme using the public key cryptosystem, and on a microcomputer. Although this scheme is inefficient because it requires duplex input of information, it will be effective if applied to only important information (*7 refs.*)
Subfile(s): B (Electrical & Electronic Engineering)
Descriptors: cryptography
Identifiers: **computer** crime; cryptography; group parity **check**; human deception; mutual surveillance; **public key** cryptosystem
Classification Codes: B6120B (Codes)
INSPEC Update Issue: 1987-004
Copyright: 1987, IEE

Dialog eLink: USPTO Full Text Retrieval Options
20/5/7 (Item 6 from file: 2)
DIALOG(R)File 2: INSPEC

03252254
Title: Authentication and digital signature
Author(s): Koyama, K.
Author Affiliation: Musashino Electrical Communication Lab., NTT, Tokyo, Japan
Journal: Information Processing Society of Japan , vol.24 , no.7 , pp.853-61
Country of Publication: Japan
Publication Date: 1983
ISSN: 0447-8053
CODEN: JOSHA4
Language: Japanese
Document Type: Journal Paper (JP)
Treatment: Practical (P)
Abstract: Computer security management has become paramount with the spread of electronic mail, office automation and other computer-integrated communication systems. It has become indispensable to automatically confirm the truth of information and the individual. This paper summarizes digital signature schemes for computer communication networks and discusses (1) identification and verification techniques for **certifying** the individual, (2) the **application** of digital signatures based on **public-key** cryptosystems, and (3) protocols for digital signatures (*28 refs.*)
Subfile(s): C (Computing & Control Engineering)
Descriptors: security of data
Identifiers: security of data; authentication; digital signature; electronic mail; office automation; computer-integrated communication systems; identification; verification techniques; public-key cryptosystems; protocols
Classification Codes: C0230 (Economic, social and political aspects of computing); C6130 (Data handling techniques)
INSPEC Update Issue: 1984-006
Copyright: 1984, IEE

B. NPL Files, Full-text

```
File  20:Dialog Global Reporter 1997-2009/Jul 13
         (c) 2009 Dialog
File  15:ABI/Inform(R) 1971-2009/Jul 11
         (c) 2009 ProQuest Info&Learning
```

```
File 610:Business Wire 1999-2009/Jul 13
        (c) 2009 Business Wire.
File 810:Business Wire 1986-1999/Feb 28
        (c) 1999 Business Wire
File 613:PR Newswire 1999-2009/Jul 13
        (c) 2009 PR Newswire Association Inc
File 813:PR Newswire 1987-1999/Apr 30
        (c) 1999 PR Newswire Association Inc
File 634:San Jose Mercury  Jun 1985-2009/Jul 10
        (c) 2009 San Jose Mercury News
File 624:McGraw-Hill Publications 1985-2009/Jul 13
        (c) 2009 McGraw-Hill Co. Inc


Set     Items   Description
S1       3532   (CONFIRM??? OR CONFIRMATION OR ACKNOWLEDG??? OR ACKNOWLEDGEMENT OR
AFFIRM??? OR ATTEST??? OR CERTIFY??? OR CHECK??? OR SUBSTANTIAT??? OR VERIFY??? OR
PROVE? ? OR PROVING OR VALIDAT??? OR AUTHENTICITY) (10N) ((PUBLIC OR PRIVATE OR
SYSTEM OR SECRET OR SYMMETRIC OR SYNCHRONOUS OR CONTENT OR ASSESS OR DECRYPTION OR
ASYMMETRIC OR SYMMETRIC)()KEY? ? OR PKI OR PGP OR WEB()TRUST)

S2        437   S1 (5N) (PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR
DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR
DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR
WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?)

S3     658269   (USAGE OR USE) (3N) (CONDITION? ? OR TERMS OR RULE? ? OR
RESTRICTION? ? OR RIGHTS OR LIMITATION? ?) OR (LIMIT??? OR RESTRICT??? OR SPECIFI??
OR PERMITTED OR FIXED OR DEFINED OR STIPULATED OR PREDEFINED OR PRESET OR
PREESTABLISHED OR PREDETERMINED) (3N) (NUMBER OR TIMES OR COPIED OR COPIES OR
PLAYED OR DOWNLOAD??) OR AVAILABILITY()DATES OR USAGE()PERIODS

S4       65430   (CRYPTOGRA? OR (ELECTRONIC OR DIGITAL)()(SEAL? ? OR SIGNATURE? ? OR
CERTIFICAT??? OR ENVELOPE? ?) OR ENCRYPT??? OR CIPHER? ? OR CYPHER? ? OR HASH?? OR
ENCOD??? OR ENC?PHER??) (10N) (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR
ART OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR
PHOTOGRAPH OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS
OR ALBUM OR ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S5     605154   (UNENCOD??? OR UNCOD??? OR UNENCRYPT??? OR DECRYPT??? OR DECOD???
OR DEC?PHER??? OR KEY OR KEYS) (10N) (MESSAGE? ? OR SIGNAL? ? OR PACKET? ? OR
TRANSMISSION? ? OR BLOCK? ? OR INFORMATION OR DATA)

S6     588285   (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR
ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR
PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR AUDIOVISUAL OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR PRODUCT OR UNIQUE OR
SECURITY) (5N) (ID OR IDS OR IDENTIFICATION OR NUMBER? ? OR IDENTIFIER? ?)

S7          0   AU=(MAARI, K? OR MAARI K? OR MAARI (1N) (K OR KOICHI))
S8          1   S2 (S) S3
S9          6   S1 (S) S3
S10         4   RD  (unique items)
```

```
S11         43   S1 (S) S4
S12         22   S11 (S) (S5 OR S6)
S13         20   RD  (unique items)
S14         20   S13 NOT (S8 OR S10)
S15          4   S14 NOT PY>1998
S16         11   S2 NOT PY>1997
S17         11   S16 NOT (S8 OR S10 OR S15)
S18         11   RD  (unique items)
```

15/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

01119888 97-69282
The Internet and EDI

Muiznieks, Vik
Telecommunications (Americas Edition) v29n11 pp: 45-48
Nov 1995
ISSN: 0278-4831 **Journal Code:** TEC
Word Count: 1387
Text:
...enhanced mail (PEM) and pretty good privacy (PGP). PEM capabilities are described in RFCs 1421 to 1424, and provide for the confidentiality of messes via **encryption**, originator authentication, **content** integrity via **message** integrity **check** (MIC) algorithms, and non-repudiation if a **public key** mechanism is used. PGP, a privately developed public/private key system, provides mechanisms for encryption and authentication.

For EDI-based security, many companies deploy firewalls...

15/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

00957574 96-06967
Cisco builds security into router software

Messmer, Ellen
Network World v11n51 pp: 17, 20
Dec 19, 1994
ISSN: 0887-7661 **Journal Code:** NWW
Word Count: 436
Text:
...secure but adds overhead," Howard noted.

Public-key technology is based on a dual-key system that matches a secret key with a publicly known **key** in order to encrypt and decrypt **data**. With **public key**, the sender's identity and **message content** can be **checked** through the **"hash"** and **digital signature.**

This technique will be supported transparently in Cisco router networks.

The particular algorithm Cisco routers will use is based on the federal government's Digital...

15/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15: ABI/Inform(R)

00908564 95-57956
Digital signatures: Signing and notarizing electronic forms

Theofanos, Mary F; Phillips, John T
Records Management Quarterly v28n2 pp: 18-22+
Apr 1994
ISSN: 1050-2343 **Journal Code:** RMQ
Word Count: 3587
Text:
...draft standards concerning the admissibility of electronic records as evidence in court. The National Institute of Science and Technology (NIST) is working to develop a **public key** encryption standard and **message** digest algorithm for use on **certifying** the authenticity of messages. The Department of the Treasury already has a system acceptable to the General Accounting Office which replaces written signatures on disbursements by using the "Data Encryption Standard (DES) to calculate a **message** digest based on a binary **key.**" Much of the **information** for this paper comes from **Data** Systems Research and Development Program efforts performed by Martin Marietta Energy Systems to develop the Prototype Electronic Records Management System (PERMS) for the U.S...

...technical issues for use of digital signatures as an additional subsystem of an overall Electronic Document Management System. The goal of the research was to **illustrate** the viability of **digital signatures** as an additional technology to existing automated records management systems and show that such a technology can provide acceptable authentication and validation similar to a...

15/3,K/4 (Item 1 from file: 813)
DIALOG(R)File 813: PR Newswire

0900048 ATTU016
SCIENTIFIC-ATLANTA LICENSES CYLINK'S SECURITY TECHNIQUES FOR DIGITAL BROADBAND APPLICATIONS

Date: January 9, 1996 12:49 EST **Word Count:** 513

Correction:
...encrypted and exchanged. The identity of
the sender and the message content can be authenticated -- an
important capability for multi-provider authorization environments and
for **validation** of orders from subscribers.
A public **key**-based cryptography system controls the encryption
and **decryption** of **messages**. Each user is assigned two unique
mathematically-related **keys**: a published public key, and a secret
private key. In a cable TV environment, the public key for each
subscriber's set-top terminal can...

18/3,K/1 (Item 1 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

01561463 02-12452

Legal reporter

Anderson, Teresa

Security Management
v41n12 pp: 127-128+

Dec 1997
ISSN: 0145-9406 **Journal**
Code: SEM
Word Count: 1973

Text:
...via the key certification system use a key escrow system that allows law
enforcement to intercept and decode encrypted communications. Under a key
certification arrangement, **computer** users obtain **public**
key certificates from some designated authority. The certificates
verify their identity, thus assuring all users of public/private
encryption keys that the private keyholders are who they claim to be. Key
certification is widely...

18/3,K/2 (Item 2 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

01500172 01-51160

Internet security: Being wired has its price

Anonymous

Computer Reseller News
n753 pp: 134-136+

Sep 8, 1997
ISSN: 0893-8377 **Journal**
Code: CRN
Word Count: 2652

Text:
...the signature is authentic and recover the message in a provably unmodified form. Signature verification is accomplished using an attached certificate.

A certificate is a **computer**-based record that **attests** to the binding of a **public key** to an identified subscriber and is issued under a specified policy. More correctly, a certificate is evidence of prior authentication, where authentication here means some...

18/3,K/3 (Item 3 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

01397342 00-48329

Smart Card advancements

Anonymous

Security
v34n3 pp: 16

Mar 1997
ISSN: 0890-8826 **Journal**
Code: SRT

Abstract:
...magnetic stripe technology. According to Kobus Marneweck, the big success story with smart cards so far has been phone cards. Another area smart cards are **proving** useful is for Internet access using **public key** encryption. In certain **applications**, such as transit cards, non-contact smart cards are where things are headed, says Marneweck.

18/3,K/4 (Item 4 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

01148649 97-98043

Digital IDs to help secure Internet

Wingfield, Nick

InfoWorld
v17n43 pp: 12

Oct 23, 1995
ISSN: 0199-6649 **Journal**
Code: IFW
Word Count: 414

Text:
...to improve Internet security by issuing digital certificates will begin next summer, when the United States Postal Service enters market testing as a digital-certificate **certifying** authority(CA).

Digital certificates are unique **programs** based on **public-key** cryptography that **verify** the identity of parties on networks such as the Internet. Certifying authorities act as trusted third parties that issue digital certificates to both end-users...

18/3,K/5 (Item 5 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

01061996 97-11390

PGP and PEM eliminate the email postcard problem

Trowbridge, Dave

Computer Technology Review
v15n6 pp: 6-12

Jun 1995
ISSN: 0278-9647 **Journal**
Code: CTN
Word Count: 1781

Text:
...and authentication are assured (assuming no one has intercepted and purposefully tampered with it). A signed message looks like gibberish, but can be read without **PGP** using a **program** that translates Radix-64 It cannot be **validated** or authenticated without **PGP**.

A signed, encrypted message cannot be read, **validated**, or authenticated without **PGP**. An unsigned, encrypted message cannot be read without PGP, but it cannot be validated or authenticated by any means--there is no assurance the message...

18/3,K/6 (Item 6 from file: 15)
DIALOG(R)File 15:
ABI/Inform(R)

00759575 94-08967

A public key extension to the Common Cryptographic Architecture

Le, An V; Matyas, Stephen M; Johnson, Donald B; Wilkins, John D
IBM Systems Journal
v32n3 pp:
461-485
1993
ISSN:
0018-8670 **Journal Code:** ISY
Word Count:
16326
Text:
...services.

The application signature generate service generates an application digital signature on the hash value of user-supplied data, using a private certification key, a **private key**-management key, or a private user key.

The **application** signature **verify** service verifies an **application** digital signature on the hash value of user-supplied data, using a public certification key, a public key-management key, or a public user key...

18/3,K/8 (Item 1 from file: 810)
DIALOG(R)File 810:
Business Wire
(c) 1999 Business Wire . All rights reserved.

0558684
BW1029

NCD SOFTWARE :
NCD Software Unveils New Integrated Security Solution for Z-Mail for Windows, Optimizing Internet Mail Protection; New ViaCrypt PGP Solution, Customized for Z-Mail, Brings Users Special Encryption, Decryption and Digital Signature Capabilities

February 20, 1996

Byline: Business Editors & Computer Writers
...attachments are secured through public-key cryptography; only the person with the corresponding private key can unlock the encrypted file.
Digital signatures, another valuable security **application** provided by ViaCrypt **PGP**, allow Z-Mail users to **verify** that the message they received was sent by a specific person and that the message was not altered.
"Security has become our customers' primary consideration...

18/3,K/9 (Item 2 from file: 810)
DIALOG(R)File 810:
Business Wire
(c) 1999 Business Wire . All rights reserved.

0486998
BW1322

CDN CREW ENERGY CORP :
CANADIAN CREW ENERGY - COMPLETION OF INITIAL GEOTHERMAL WELL ANTICIPATED BY EARLY JUNE - PROJECT REVIEW

May 15, 1995

Byline: Business Editors
...about 1300 metres then angled towards Meager Mountain to two target zones, at depths of about 2400 metres and about 3450 metres.
The exploration drilling **program** has been designed to **confirm** assumptions that Pacific GeoPower **(PGP)** (a joint venture between

Canadian Crew Energy Corp. and Guy F. Atkinson Holdings) has made about the temperature, flow rates, geological structure, and other aspects...

18/3,K/10 (Item 3 from file: 810)
DIALOG(R)File 810:
Business Wire
(c) 1999 Business Wire . All rights reserved.

0476511
BW1052

COMMERCENET :
CommerceNet Launches Comprehensive Certification Model For Commercial Use On The Internet Certification Authority Pilot Provides Critical Stage in Assuring Secure Internet Electronic Commerce

April 10, 1995

Byline:
Business Editors/Computer Writers
...technology to certify secure web servers and CommerceNet-affiliated individuals engaged in electronic commerce pilots over the Internet. By positively identifying buyers and sellers through **public key** certificates and other **proven** security technology, the **program** will provide a major step in providing the assurance needed for the Internet to be used for commercial transactions.
"This trial is a major step...

18/3,K/11 (Item 1 from file: 634)
DIALOG(R)File 634: San Jose Mercury
(c) 2009 San Jose Mercury News. All rights reserved.

07642177

GOVERNMENT, FIRMS FIND WAY TO VERIFY ELECTRONIC SIGNATURES

San Jose Mercury News (SJ) - Saturday, May 21, 1994
By:
Associated Press
Edition: Morning Final
Section: Business **Page:** 13D
Word Count:

...retrieved by the agency, a 320-bit number, which is the electronic signature, will appear on the document. The government employee will then run a **computer program** to **verify** the signature against the person's **public key**. The key could be stored in a secure government data base, Smid said.

File 9:Business & Industry(R) Jul/1994-2009/Jul 11
(c) 2009 Gale/Cengage
File 275:Gale Group Computer DB(TM) 1983-2009/Jun 12
(c) 2009 Gale/Cengage
File 621:Gale Group New Prod.Annou.(R) 1985-2009/Jun 04
(c) 2009 Gale/Cengage
File 636:Gale Group Newsletter DB(TM) 1987-2009/Jun 18
(c) 2009 Gale/Cengage
File 16:Gale Group PROMT(R) 1990-2009/Jun 18
(c) 2009 Gale/Cengage
File 160:Gale Group PROMT(R) 1972-1989
(c) 1999 The Gale Group
File 148:Gale Group Trade & Industry DB 1976-2009/Jun 25
(c) 2009 Gale/Cengage

Set Items Description
S1 5252 (CONFIRM??? OR CONFIRMATION OR ACKNOWLEDG??? OR ACKNOWLEDGEMENT OR AFFIRM??? OR ATTEST??? OR CERTIFY??? OR CHECK??? OR SUBSTANTIAT??? OR VERIFY??? OR PROVE? ? OR PROVING OR VALIDAT??? OR AUTHENTICITY) (10N) ((PUBLIC OR PRIVATE OR SYSTEM OR SECRET OR SYMMETRIC OR SYNCHRONOUS OR CONTENT OR ASSESS OR DECRYPTION OR ASYMMETRIC OR SYMMETRIC)()KEY? ? OR PKI OR PGP OR WEB()TRUST)

S2 575 S1 (5N) (PLAYER OR PLAYERS OR RECORDER OR RECORDERS OR PLAYBACK OR DEVICE OR DEVICES OR VCR OR VCRS OR DVDR OR DVDRS OR APPARATUS OR DVR OR DIGITAL()VIDEO()RECORDER? ? OR PC OR PCS OR COMPUTER? ? OR DESKTOP? ? OR WORKSTATION? ? OR PROGRAM? ? OR APPLICATION? ? OR MODULE? ?)

S3 520145 (USAGE OR USE) (3N) (CONDITION? ? OR TERMS OR RULE? ? OR RESTRICTION? ? OR RIGHTS OR LIMITATION? ?) OR (LIMIT??? OR RESTRICT??? OR SPECIFI?? OR PERMITTED OR FIXED OR DEFINED OR STIPULATED OR PREDEFINED OR PRESET OR PREESTABLISHED OR PREDETERMINED) (3N) (NUMBER OR TIMES OR COPIED OR COPIES OR PLAYED OR DOWNLOAD??) OR AVAILABILITY()DATES OR USAGE()PERIODS

S4 100470 (CRYPTOGRA? OR (ELECTRONIC OR DIGITAL)()(SEAL? ? OR SIGNATURE? ? OR CERTIFICAT??? OR ENVELOPE? ?) OR ENCRYPT??? OR CIPHER? ? OR CYPHER? ? OR HASH?? OR ENCOD??? OR ENC?PHER??) (10N) (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?) OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR AUDIOVISUAL)

S5 631203 (UNENCOD??? OR UNCOD??? OR UNENCRYPT??? OR DECRYPT??? OR DECOD??? OR DEC?PHER??? OR KEY OR KEYS) (10N) (MESSAGE? ? OR SIGNAL? ? OR PACKET? ? OR TRANSMISSION? ? OR BLOCK? ? OR INFORMATION OR DATA)

```
S6      465945   (CONTENT OR IMAGE OR IMAGES OR PICTURE OR PICTURES OR ART OR
ARTWORK? ? OR GRAPHIC OR GRAPHICS OR ILLUSTRAT? OR PHOTO OR PHOTOS OR PHOTOGRAPH OR
PHOTOGRAPHS OR PHOTOGRAPHY OR MOVIE? ? OR FILM? ? OR VIDEO OR VIDEOS OR ALBUM OR
ALBUMS OR TRACK OR TRACKS OR MP3 OR MP3 MP()3 OR (MPEG()1 OR
MPEG1)()AUDIO()LAYER()3 OR GAME OR GAMES CD OR CDS OR COMPACT()(DISK? ? OR DISC? ?)
OR AUDIOVISUAL OR DVD OR DVDS OR MUSIC OR SONG OR SONGS OR PRODUCT OR UNIQUE OR
SECURITY) (5N) (ID OR IDS OR IDENTIFICATION OR NUMBER? ? OR IDENTIFIER? ?)

S7           0   AU=(MAARI, K? OR MAARI K? OR MAARI (1N) (K OR KOICHI))
S8           0   S2 (S) S3
S9          21   S2 AND S3
S10         12   RD  (unique items)
S11          1   S10 NOT PY>1997
S12         15   S1 (S) S3
S13          7   RD  (unique items)
S14        105   (S1 OR S2) (S) S4
S15         41   S14 (S) (S5 OR S6)
S16         10   S15 NOT PY>1997
S17          8   RD  (unique items)
S18        141   S1 AND S3
S19        132   S18 NOT (S11 OR S13 OR S17)
S20         35   S19 NOT PY>1997
S21         29   RD  (unique items)
```

11/3,K/1 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02097007 **Supplier Number:** 19656448 **(Use Format 7 Or 9 For** FULL TEXT)
Time to spend electronic money. (e-commerce issues for businesses) (Internet/Web/Online Service Information)

Kessler, Gary; Sheppard, Steve
Network VAR , v5 , n8 , p65(8)
August , 1997
ISSN: 1082-8818
Language: English **Record Type:** Fulltext; Abstract
Word Count: 5177 **Line Count:** 00468

```
...and unique identifier
     Validity (or operational) period
     Subject's name and unique identifier
     Subject's public key information
     Standard extensions
        Certificate appropriate U# definition
        Key usage limitation definition
        Certificate policy information
     Other extensions
        Application-specific
        Certificate authority (CA)-specific
      A certificate authority (CA), then, is any agency that issues
certificates. A company...

...begs for a formal definition. While electronic commerce, and commerce
over the Internet in particular, is a motivating factor for PKI and CA
work, the applications for PKI are much broader. PKI
applications include secure electronic mail, payments and electronic
checks, electronic data interchange (EDI), secure transfer of domain
```

name service (DNS) and routing information, electronic forms, and digitally signed documents.
While a single global PKI...

17/3,K/2 (Item 1 from file: 275)
DIALOG(R)File 275: Gale
Group Computer DB(TM)
(c) 2009 Gale/Cengage. All rights reserved.

01868535 **Supplier Number:**
17610992 **(Use Format 7 Or 9 For** FULL TEXT)

The Internet and EDI. (electronic data interchange) (Technology Information)

Muiznieks, Vik

Telecommunications , v29 , n11 , p45(3)

Nov , 1995
ISSN: 0278-4831
Language:
English **Record Type:** Fulltext; Abstract

Word Count: 1533 **Line Count:** 00139
...enhanced mail (PEM) and pretty good privacy (PGP). PEM capabilities are described in RFCs 1421 to 1424, and provide for the confidentiality of messages via **encryption**, originator authentication, **content** integrity via **message** integrity **check** (MIC) algorithms, and non-repudiation if a **public key** mechanism is used. PGP, a privately developed public/private key system, provides mechanisms for encryption and authentication.
For EDI-based security, many companies deploy firewalls...

17/3,K/3 (Item 2 from file: 275)
DIALOG(R)File 275: Gale
Group Computer DB(TM)
(c) 2009 Gale/Cengage. All rights reserved.

01032028 **Supplier Number:**
00522323
Digital Signatures: A Tutorial Survey.

Akl, S.G.

Computer , v16 , n2 , p15-24

Feb. , 1983

ISSN: 0018-9162
Language:
ENGLISH **Record Type:** ABSTRACT

Abstract: For various reasons it is desirable in electronic mail systems to **validate** and authenticate **message content.** In public and private- **key** cryptosystems a **digital signature** that is appended to or integrated into a message can assure that a sender's (S) message is received only by the receiver (R) and... ...S. Although relatively slow, a system such as the Rivest-Shamir-Adleman (RSA) system that uses two random 100 decimal digit numbers to generate a **key** assures **message** integrity. By using the best known algorithm calculating the **key** would take over a billion years of computing time.
Abstract:

17/3,K/4 (Item 1 from file: 636)
DIALOG(R)File 636: Gale
Group Newsletter DB(TM)
(c) 2009 Gale/Cengage. All rights reserved.

02977714 **Supplier Number:**
46068965 **(USE FORMAT 7 FOR FULLTEXT)**

SCIENTIFIC-ATLANTA: S-A licenses Cylink's security techniques for digital broadband applications
M2
Presswire , p N/A
Jan 16 , 1996

Language: English **Record Type:** Fulltext

Document Type: Newswire ; Trade
Word Count:
547
-
...encrypted and exchanged. The identity of the sender and the message content can be authenticated -- an important capability for multi-provider authorisation environments and for **validation** of orders from subscribers.
A public **key**-based cryptography system controls the encryption and **decryption** of **messages.** Each user is assigned two unique mathematically-related **keys:** a published public key, and a secret private key. In a cable TV environment, the public key for each subscriber's set-top terminal can...

17/3,K/5 (Item 2 from file: 636)
DIALOG(R)File 636: Gale

Group Newsletter DB(TM)
(c) 2009 Gale/Cengage. All rights
reserved.

02532509 **Supplier Number:**
45104635 **(USE FORMAT 7 FOR FULLTEXT)**

Security of paper-based systems

Financial Technology Insight , p N/A

Nov , 1994
Language:
English **Record Type:** Fulltext
Document Type:
Newsletter ; Trade
Word Count: 122

**Supplier Number: (USE
FORMAT 7 FOR FULLTEXT)**

Text:
A **digital** signature is essentially a very complex checksum, related to the **content** of the **message** and a **number** (the private **key**) known only to the sender. A different, but related, number (the **public key**) allows the recipient to **check** who sent the **message**. In order to tie these **keys** back to a particular organization or individual, it is possible to issue a credit card -sized token, called a smartcard. This contains a tiny computer...

17/3,K/6 (Item 1 from file: 148)
DIALOG(R)File 148: Gale
Group Trade & Industry DB
(c) 2009 Gale/Cengage. All rights
reserved.

08016758 **Supplier Number:**
17221232 (USE FORMAT 7 OR 9 FOR FULL TEXT)

VeriSign to offer digital ID services.

Roberts, Erica

CommunicationsWeek , n563 , p4(1)

June 26 , 1995
ISSN: 0746-8121
Language:
English
Record Type: Fulltext; Abstract
Word Count:

323 **Line Count:** 00029

Abstract: ...difficult to assess validity of information received over the network and is difficult to verify sources. On-line service providers, he says, need to provide **content** integrity and **validation** of services. VeriSign employs **public-key cryptography**, which uses a matched pair of public and private **keys** to encrypt and **decrypt messages.**
Abstract:

17/3,K/7 (Item 2 from file: 148)
DIALOG(R)File 148: Gale
Group Trade & Industry DB

06796891 **Supplier Number:**
14023755 (USE FORMAT 7 OR 9 FOR FULL TEXT)

NIST's 'victory' will save DSS users an arm and a leg.
(National Institute of Standards and Technology, digital signature standard) (IRM Notebook) (Column)

Houser, Walter R.

Government Computer News , v12 , n14 ,
p25(1)
July 5 , 1993
Document Type: Column

ISSN: 0738-4300
Language: ENGLISH
Record Type:
FULLTEXT; ABSTRACT
Word Count: 815
Line Count: 00064
...key for decoding. The agency application system uses its private key and the citizen's public key to code the messasge so it can be **decoded** only by the intended recipient.
Even when the message **content** is not sensitive, **public-key** algorithms can serve as digital **signatures**, ensuring the **authenticity** and integrity of messages. A sender's mail software can "sign" messages by encrypting a "hash" number calculated by running the text though a standard...

17/3,K/8 (Item 3 from file: 148)
DIALOG(R)File 148: Gale
Group Trade & Industry DB

reserved.

06181289 **Supplier Number:**
13035397 (USE FORMAT 7 OR 9 FOR FULL TEXT)

Changes to encryption standard would expand fed users' options.
(Federal Information Processing Standard 46-1 for the Data Encryption Standard)
(Brief Article)

Schwartz, Karen D.

Government Computer News , v11 , n24 ,
p3(1)
Nov 23 , 1992
Document Type: Brief
Article
ISSN: 0738-4300
Language: ENGLISH
Record Type:
FULLTEXT
Word Count: 352
Line Count: 00028
...DES revision more consistent with the proposed FIPS for digital signatures. The Digital Signature Standard, now in a second public comment period, will specify a **public-key digital signature** algorithm and allow users to **verify** both **message content** and sender identity.
So far, most agency comments seem to favor renewing DES as is, Smid said, but he has received verbal requests to add...

01454886 Supplier Number: 24101284 **(USE FORMAT 7 OR 9 FOR FULLTEXT)**
Tales from the encryption
(Problems with early copy protection systems impeded their widespread adoption, but large scale commercial software piracy has spurred new interest in finding effective ways to halt this drain on revenues)

One to One , n 89 , p 51
December 1997
Document Type: Journal **ISSN:** 0268-8786 (United Kingdom)
Language: English **Record Type:** Fulltext
Word Count: 3292 **(USE FORMAT 7 OR 9 FOR FULLTEXT)**

TEXT:
...information, CD-Secure2 can also define exactly what conditions the software can be used under. It could be try-before-you-buy - offering 30 days **usage** without **restriction** before the disc becomes useless unless it is 'bought' with a credit card - or, using pay-as-you-go options, it can control the number...

...per copy. Ideally, the replicator needs the CD-Cops disc analysis software that provides the original keycode information so that the first discs can be **checked** off the line and the final **public**

key code generated quickly ready for label printing. With just a few hours turnaround to produce the public keycode, the delays introduced by CD-Cops are...

21/3,K/2 (Item 1 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02118629 **Supplier Number:** 19958165 **(Use Format 7 Or 9 For** FULL TEXT)
Open for business: Web storefront creation software. (12 electronic-commerce products reviewed) (includes related articles on elements of an electronic storefront, Editors' Choices, glossary, online-service and ISP templates, offering transaction security, business-to-business commerce) (Software Review)(Evaluation)

Linthicum, David S.
PC Magazine , v16 , n20 , p143(19)
Nov 18 , 1997
Document Type: Evaluation
ISSN: 0888-8507
Language: English **Record Type:** Fulltext; Abstract
Word Count: 12518 **Line Count:** 00996
...data security and interoperability between payment schemes.
Public-key encryption An encryption system that uses two keys, a public key for encrypting messages and a **private key** for decrypting messages, to enable users to **verify** each other's messages without exchanging **secret keys.**
Secure Electronic Transaction (SET) A secure payment protocol developed by MasterCard and Visa designed to ensure security for bank card transactions over the Internet. It...

...A public security protocol, also developed by Netscape, that can create a secure link between the Web server and the browser.
SKU Stockkeeping unit; a **number** designating one **specific** product.
Taxware A software program, developed by Taxware International, that provides detailed tax rate information to commerce servers over the Internet.
Virtual Spin LLC: Cartalog...

21/3,K/3 (Item 2 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02060529 **Supplier Number:** 19365954 **(Use Format 7 Or 9 For** FULL TEXT)
Role of digital certificates looks secure; but roadblocks to use include no interoperability, too many issuing authorities. (Technology Information)

Kosiur, Dave
PC Week , v14 , n17 , p115(2)
April 28 , 1997
ISSN: 0740-1604

Language: English **Record Type:** Fulltext; Abstract
Word Count: 1506 **Line Count:** 00124
...A sender can generate a digital signature for a message using a private key, but recipients of the signed message need the sender's corresponding **public key** to **verify** the digital signature. Obtaining a copy of the sender's digital certificate is one way of doing this.
Corporations also can issue digital certificates to...
...or CAs, will verify each other's certificates as more issuers join the marketplace and more people use digital certificates. Right now, there are a **limited number** of well-known, trusted CAs, including but not limited to the U.S. Postal Service, VeriSign and Entrust Technologies Inc., but the number will grow...

21/3,K/4 (Item 3 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

02049612 **Supplier Number:** 19055885 **(Use Format 7 Or 9 For** FULL TEXT)
E-mail programs. (SoftArc's FirstClass 3.5, StarNine Technologies' Quarterdeck Mail 4.0 and CE Software's QuickMail Pro) (Software Review)(Evaluation)

Beckman, Mel
Macworld , v14 , n3 , p48(2)
March , 1997
Document Type: Evaluation
ISSN: 0741-8647
Language: English **Record Type:** Fulltext; Abstract
Word Count: 1346 **Line Count:** 00113
...by the "seat," or user, license control is an important issue--particularly if you're setting up man y users. A license key gives a **specific number** of users access to the server, allowing the programs to be distributed over a network. All three products have thorough end-user documentation, but only...

...interserver message routing, batch account administration, and Internet interoperability. Users want styled text, forms processing, automatic replies, dra g-and-drop attachment handling, a spelling **checker**, **public-key** encryption, and rule-driven filtering.
On the server side, both Quarterdeck Mail and FirstClass have competent backup mechanisms, routing between message servers, and batch account...

21/3,K/5 (Item 4 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01997529 **Supplier Number:** 18741144 **(Use Format 7 Or 9 For** FULL TEXT)
Web servers. (Lab Test) (includes related articles on the top products, Netscape Enterprise 2.0 and FTP Esplanade for Windows NT, and on Apple's Internet Server Solution)(Evaluation)

PC User , n289 , p50(14)

August 21 , 1996
Document Type: Evaluation
ISSN: 0263-5720
Language: English **Record Type:** Fulltext; Abstract
Word Count: 10664 **Line Count:** 00828
...of clients on the network increased. Efficient servers should follow an upward trend, until the maximum number of connections is reached. Lower-specification products which **limit** the **number** of concurrent connections start off with a poor score and rapidly get worse.

Microsoft Internet Information Server 1.0 and Netscape's Enterprise 2.0...Internet with just a user name and password, and demonstrates the benefits of applications using HTML and JavaScript. However, the whole system feels cumbersome and **limited.** At **times** response is slow, and viewing at 640x480 resolution tends to be cramped. Despite this, the interface is easy to use and allows access to every...the private key. Any message encrypted with the server's private key and the client's public key can be decrypted using the client's **private key** and the server's **public key.**

Checking sender ID

Another feature offered with SSL is the ability to check the identity of the sender of a message. This doesn't encrypt the message, but still creates an exclusive channel between the server and client, where the message can be digitally signed. This signature is again **confirmed** using the **public key** system.

The SSL protocol requires server administrators to obtain a Key Certificate from a certificate authority, which maintains a list of authorised certificate holders and...

21/3,K/7 (Item 6 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01861496 **Supplier Number:** 17433068 **(Use Format 7 Or 9 For** FULL TEXT)
Defending the Unix perimeter. (poor Unix administration can render networks vulnerable to security threats)(includes related articles)(Special Report) (Technology Tutorial)(Tutorial)

Cullen, Cindy
LAN Magazine , p149(3)
Oct , 1995
Document Type: Tutorial
ISSN: 1069-5621
Language: English **Record Type:** Fulltext; Abstract
Word Count: 2587 **Line Count:** 00204
...The windowing standard for Unix is X Window. It is usually referred to as X. Security for X is controlled by the end user. The **use** of the **terms** client and server can be confusing in relation to X; for clarity, the monitor displaying X will be called a display station. The user can...legitimate receiver can decrypt the message with their private key.

Each user's private key can be used to digitally sign a document. The corresponding **public key** is used to **verify** that the document was written by the author and hasn't been tampered with.

PGP is freeware for noncommercial use, although commercially supported versions do...

21/3,K/8 (Item 7 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01802864 **Supplier Number:** 17162300 **(Use Format 7 Or 9 For** FULL TEXT **)**
Making your customer's network secure.

Addelson, Roger
STACKS , v2 , n12 , p27(7)
Dec , 1994
ISSN: 1070-8596
Language: English **Record Type:** Fulltext; Abstract
Word Count: 4120 **Line Count:** 00341
...protection is automatic callback. Again, based upon an ID/password combination, the communication program gracefully disconnects the session, then calls the user back at a **predetermined** phone **number** associated with the ID/password. This requires that the remote user call from a prearranged phone number. It is particularly cumbersome for remote users who...
...the administrator to restrict the time, day, and specific workstation location from which a particular user may access the network resources.
Intruder-detection schemes often **restrict** the **number** of incorrect login attempts associated with an ID. If a **preset number** of incorrect attempts occurs within a specified period of time, the account is disabled or the workstation is locked for a predetermined period and a...create a digital envelope, which holds an RSA-encrypted DES key and DES-encrypted data. You can create a digital signature as a means of **verifying** who you are by encrypting with your **private key** and letting others decrypt your message with your public key.
Congress and the Clinton Administration have proposed a controversial new encryption device called the Clipper...

21/3,K/9 (Item 8 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01801703 **Supplier Number:** 17162680 **(Use Format 7 Or 9 For** FULL TEXT **)**
Toward electronic money: some Internet experiments. (includes related articles on RSA's public-key encryption and on smart cards for digital money)

Dyson, Peter E.
Seybold Report on Desktop Publishing , v9 , n10 , p3(9)
June 10 , 1995
ISSN: 0889-9762
Language: English **Record Type:** Fulltext
Word Count: 6493 **Line Count:** 00607
...all the proposals for digital money. But encryption by itself cannot create trust. It can only transfer distrust. For example, it is said that a **public-key** signature can unambiguously **verify** the

identity of the sender of a message. But that presumes that the public key truly identifies the right person. You must then ask how...bank might use one key for one-dollar coins, another for five- dollar coins and so on. The bank would, of course, publish the corresponding **public keys**, allowing anyone to **verify** the value of such a coin. When the Pay button for an Internet purchase is pressed, your computer contacts the bank and asks to download...process of guessing at factors rather unrewarding. On the other hand, testing whether a given number is prime is fairly easy, and there is no **limit** to the **number** of primes that exist.

In the RSA scheme, encryption keys are large prime numbers, and are always chosen in pairs. (By large, we mean at...

...key. Thus it is possible to publish one of the keys, provided you keep the other one secret.

There are two main uses for a **public-key** encryption system: sending secret messages and **proving** your identity. They use the public and **private keys** in opposite ways:

To send a message that only the intended recipient can decode, you look up his public key in a directory. (On the...

21/3,K/10 (Item 9 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01695703 **Supplier Number:** 16192274 **(Use Format 7 Or 9 For** FULL TEXT)
Cyber-privacy: in cyberspace, the walls have ears. So check out the RSAREF cryptography toolkit and keep your E-mail safe. (RSA Data Security Inc) (Tutorial)

Lane, Alex
Computer Shopper , v14 , n9 , p594(3)
Sept , 1994
Document Type: Tutorial
ISSN: 0886-0556
Language: ENGLISH **Record Type:** FULLTEXT; ABSTRACT
Word Count: 2305 **Line Count:** 00178
...you to encrypt the message with your private key as well, so that upon receipt the message will only become readable when decrypted with your **public key**, thus **proving** you sent the message.

Message Digests and Data Signatures

Just as a fingerprint identifies a person, a message digest can be used to verify data...math performed in RSAREF makes heavy use of large prime numbers, so large that most programming languages can't handle them. A 1,024-bit **number** (the maximum size **defined** for an RSA modulus) occupies 128 bytes! Such components of public- and private-key structures are stored in fixed-length arrays of unsigned characters with...

21/3,K/11 (Item 10 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01673167 **Supplier Number:** 15084249 **(Use Format 7 Or 9 For** FULL TEXT)

RSA opens up security technology. (RSA Data Security Inc.) (Brief Article)

Hess, Robert
MacWEEK , v8 , n13 , p15(1)
March 28 , 1994
Document Type: Brief Article
ISSN: 0892-8118
Language: ENGLISH **Record Type:** FULLTEXT
Word Count: 249 **Line Count:** 00020

...sender. A user with a private Ripem key -- similar to a very long, nonsensical password -- can sign a message so that anyone with the associated **public key** can **verify** the identity of the originator. Apple uses this technology to ensure the reliability of PowerShare and PowerTalk communications.

RSA previously distributed a freeware reference implementation of its cryptographic tools, but, until now, this software was approved only for individual use. Now the company has relaxed **restrictions** and allows **use** within any custom application, as long as the resulting product is not sold or used to provide a for-profit service.

Ripem code is available...

21/3,K/12 (Item 11 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01616858 **Supplier Number:** 14352102 **(Use Format 7 Or 9 For** FULL TEXT)
To catch a thief. (Network Edition) (network security)(includes related article on securing NetWare 3.11)

Derfler, Frank J. Jr.; Schireson, Max; Stefanini, Tim
PC Magazine , v12 , n16 , pNE1(5)
Sept 28 , 1993
ISSN: 0888-8507
Language: ENGLISH **Record Type:** FULLTEXT; ABSTRACT
Word Count: 2724 **Line Count:** 00226

...each 512 bits long. The public and private numbers are mathematically related so that data is encrypted using the private key and decrypted using the **public key**. This makes it possible to **verify** exactly who sent the encrypted information. RSA is considered nearly impervious to brute force attack. It is based on factoring extremely large numbers, which requires...primarily protect a system from break-in attempts based on repeated trials of password cracking. The following are Novell's guidelines:

Recommended default account balance/**restrictions**: (**use** default)
Account has expiration date: no
Date account expires: (use default)
Limit concurrent connections: yes
Maximum connections: 1
Require password: yes
Minimum password length: 5...

21/3,K/13 (Item 12 from file: 275)
DIALOG(R)File 275: Gale Group Computer DB(TM)

01615373 **Supplier Number:** 14207743 **(Use Format 7 Or 9 For** FULL TEXT)
Communications privacy: implications for network design.

Rotenberg, Marc
Communications of the ACM , v36 , n8 , p61(8)
August , 1993
ISSN: 0001-0782
Language: ENGLISH **Record Type:** FULLTEXT; ABSTRACT
Word Count: 7065 **Line Count:** 00594
...forms of protection establish rights that are enforceable in law. These rights typically allow for the recoupment of damages from private parties, criminal fines, or **restrictions** on the **use** of the unlawfully gathered information where the transgression occurs by the government.

Legal protections are likely to clarify the underlying privacy interests, but are ...A related use for cryptography is the authentication of messages. Using public key encryption, a user can encrypt a message using his or her own **private key.** The recipient of the message can then determine the **authenticity** of the messages by using the sender's **public key.**

To be effective, standards must be established so that users in different networks will be able to exchange messages. Anything less than a full implementation...

...are collected should be specified not later than at the time of data collection and the subsequent use should be limited to those purposes.

* The **Use Limitation** Principle states that personal data should not be disclosed for secondary purposes except with the consent of the data subject or by authority of law...the service, detailed profiles on users could be developed.

Regulatory authorities in the U.S. and Canada generally favored this second view and recommended strong **restrictions** on the **use** of the service. The policy debate surrounding Caller ID, and questions regarding the disclosure of personal data, are likely to continue as the service is...

21/3,K/14 (Item 1 from file: 621)
DIALOG(R)File 621: Gale Group New Prod.Annou.(R)

01485061 **Supplier Number:** 47100154 **(USE FORMAT 7 FOR FULLTEXT)**
Security Dynamics Announces Third-Generation ACE/Serverr.

Business Wire , p 02041269
Feb 4 , 1997
Language: English **Record Type:** Fulltext
Document Type: Newswire ; Trade
Word Count: 1604

...introduce products and form partnerships that will enable delivery of the following security services:

-- Certificate Management - Security Dynamics believes that in the future, certificates, which **attest** to the **authenticity** of the owners of **public keys**, will be increasingly used for identification and authentication, digital signatures and to support secure email (S/MIME), secure browser communications (with SSL) and secure communications over the Internet (S/WAN). A certificate authority (CA) serves as a trusted third party that vouches for the **authenticity** of owners of **public keys**.

As part of its ESS certificate services, Security Dynamics plans to simplify the management of diverse certificates. Specifically, Security Dynamics intends to offer a software...accessible through Web browsers, to manage all Enterprise Security Services.

"The ESS architecture is providing our customers with a framework for understanding how public and **private key**, certificates, and other encryption technologies will be deployed on a **proven** security platform - ACE/Server - to deliver real corporate security applications," said Dave Power.

Pricing and Availability

Version 3.0 of the ACE/Server is currently...

...development, undetected software errors or bugs, changes in product pricing policies, competitive pressures, technical difficulties, market acceptance of the new products and technologies, including without **limitation** the **use** and implementation of various certificate management and key management technologies, changes in customer requirements and government regulations, delays in developing strategic partnerships, general economic conditions...

21/3,K/17 (Item 2 from file: 636)
DIALOG(R)File 636: Gale Group Newsletter DB(TM)

01072148 **Supplier Number:** 40664720 **(USE FORMAT 7 FOR FULLTEXT)**

ELECTRONIC DATA INTERCHANGE, OPEN NETWORKS AND BUSINESS SECURITY
Computer Fraud & Security Bulletin , v 11 , **n** 4 , p N/A
Feb , 1989
Language: English **Record Type:** Fulltext
Document Type: Newsletter ; Trade
Word Count: 3847

...and then compared with the stored form. Matching results in the EDI service being made available, but mismatch terminates the log-on. There is a **limit** set to the **number** of log-on retries which may be made before all further attempts are barred and network services staff alerted.

These network services staff follow a...for the data transmission session. The message's digital signature is encrypted using A's private key, and decrypted by recipient B using A's **public key**, which has been sent to him.

Successful decryption **proves** not only the integrity of the entire EDI message but also that the private key, held by A, is the only key that could have...factor on the adoption of EDI; legal rules of evidence may be less than ideal while not intentionally forming a barrier to progress. The wide **use** of the UNCID **rules** should be of

great benefit in allowing parties to foresee and forestall potential problems.
As use of EDI grows there will be an increasing need...

21/3,K/19 (Item 2 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

04993074 **Supplier Number:** 47333550 **(USE FORMAT 7 FOR FULLTEXT)**

Role of Digital Certificates Looks Secure; But roadblocks to use include no interoperability, too many issuing authorities
Kosiur, Dave
PC Week , p 115
April 28 , 1997
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal; Tabloid ; General Trade
Word Count: 1412
-
...A sender can generate a digital signature for a message using a private key, but recipients of the signed message need the sender's corresponding **public key** to **verify** the digital signature. Obtaining a copy of the sender's digital certificate is one way of doing this.
Corporations also can issue digital certificates to...

...or CAs, will verify each other's certificates as more issuers join the marketplace and more people use digital certificates. Right now, there are a **limited number** of well-known, trusted CAs, including but not limited to the U.S. Postal Service, VeriSign and Entrust Technologies Inc., but the number will grow...

21/3,K/20 (Item 3 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

04544262 **Supplier Number:** 46678243 **(USE FORMAT 7 FOR FULLTEXT)**

The key to security
InfoWorld , p 01
Sept 2 , 1996
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal ; Trade
Word Count: 2677
-
...mathematically different implementation of the asymmetrical model, and it is the method employed by DSN's NetFortress.
THE REAL YOU. Using public or public and **private keys** is the foundation of encryption, but keys can't **verify** a recipient's identity.
"When you're talking about sending secured messages, there are two goals you've got. One is to make sure that...Era Act of 1996 also sits

before the Senate.
     All three laws would relax the 40-bit restriction on keys as well as eliminate other **restrictions** on international **use** and development of encryption.
     Officials of U.S. corporations look forward to these changes and believe that such changes would improve their ability to compete...

21/3,K/21 (Item 4 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

04422462 **Supplier Number:** 46488417 **(USE FORMAT 7 FOR FULLTEXT)**

Livermore Labs, Bank of America debut secure EDI
PC Week , p 010
June 24 , 1996
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal; Tabloid ; General Trade
Word Count: 490

...s success in making "cash" transactions over the Internet, the commercial product that may emerge from the endeavor could have a leg up on the **limited number** of EDI applications already on the market.
     Potential competitors include Premenos Corp., Harbinger Corp., General Electric Information Services Inc., Sterling Commerce Inc. and Electronic Commerce...

...which uses RSA Security Inc.'s dual-key cryptography algorithms in conjunction with standard MIME (Multipurpose Internet Mail Extension). The RSA algorithms use public and **private keys.**
     The process starts with Livermore Labs' MIC (Message Integrity **Check**). The MIC is encrypted with the labs' **private key,** and the encrypted MIC is embedded in the Internet E-mail message as a MIME attachment.
     The process automatically produces a DES (Digital Encryption Standard ...

21/3,K/22 (Item 5 from file: 16)
DIALOG(R)File 16: Gale Group PROMT(R)

03701807 **Supplier Number:** 45240798 **(USE FORMAT 7 FOR FULLTEXT)**

Making Security A Reality For All
InformationWeek , p 38
Jan 2 , 1995
Language: English **Record Type:** Fulltext
Document Type: Magazine/Journal; Tabloid ; General Trade
Word Count: 1515

...Reynolds, a senior consultant with EDS Corp.'s management-consulting

services in Plano, Texas. One answer is to create some kind of certification authority to **validate public keys** and to issue certificate revocation lists if a key is lost or stolen. Digital certificates - documents that vouch for the ownership of a public key...

...might be a continent away. Cyber notaries could approve the certification and allow the deal to proceed under an umbrella of trust. 'We're creating **rules** for the **use** of certification authorities,' says Baum.
No one knows what impact the Republican Party's sweep of Congress will have on either Clipper or the government...

21/3,K/23 (Item 1 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

09500797 **Supplier Number:** 19437891 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Ordering by E-mail. (Internet Tips)(includes related glossary of Internet buzzwords) (Internet/Web/Online Service Information)

Heim, Judy
PC World , v15 , n6 , p286(2)
June , 1997
ISSN: 0737-8939
Language: English
Record Type: Fulltext
Word Count: 1579 **Line Count:** 00124
...you may receive with each piece of e-mail, receipt and delivery can be slow. Some of the services permit you to receive only a **limited number** of messages each week, and some may store waiting mail on the service for only a week, then delete it. Also, while these services say...

...The character string is a calculation based on the sender's secret key and the contents of the message. To authenticate a message, the recipient **checks** it with the sender's **public key.**
Encryption. The process of encoding a document so others can't read it.
Keys. In the RSA scheme, you use a public key and a...

21/3,K/24 (Item 2 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

08937535 **Supplier Number:** 18643471 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The key to security. (includes related article on exporting encryption) (Technology Information)

Bort, Julie
InfoWorld , v18 , n36 , p1(3)
Sep 2 , 1996
ISSN: 0199-6649
Language: English

Record Type: Fulltext; Abstract
Word Count: 2780 **Line Count:** 00223
...mathematically different implementation of the asymmetrical model, and it is the method employed by DSN's NetFortress.

THE REAL YOU. Using public or public and **private keys** is the foundation of encryption, but keys can't **verify** a recipient's identity.

"When you're talking about sending secured messages, there are two goals you've got. One is to make sure that...Era Act of 1996 also sits before the Senate.

All three laws would relax the 40-bit restriction on keys as well as eliminate other **restrictions** on international **use** and development of encryption.

Officials of U.S. corporations look forward to these changes and believe that such changes would improve their ability to compete...

21/3,K/25 (Item 3 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

08753456 **Supplier Number:** 18371288 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Data security: key issue in an age of pervasive computing.(Cover Story)

Strassberg, Dan
EDN , v41 , n8 , p48(7)
April 11 , 1996
Document Type: Cover Story
ISSN: 0012-7515
Language: English
Record Type: Fulltext; Abstract
Word Count: 4164 **Line Count:** 00334
...writing in which units of plain text are substituted according to a predetermined key, the key to such a system, or a ciphered message." Cryptographers **use** the **terms** "plaintext" and "cipher-text" to refer to the content of messages before and after encryption.

Although encryption dates back at least to the Middle Ages...Such modifications and forgeries are more difficult with these protocols than with handwritten signatures.

Still, message originators can disavow digital signatures. Someone who uses his **secret key** to encrypt a message and thus guarantee the message's **authenticity** can claim that, before he encrypted the message, a third party gained access to the key without his knowledge. The originator can claim that he...

21/3,K/26 (Item 4 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

08298180 **Supplier Number:** 17610992 (USE FORMAT 7 OR 9 FOR FULL TEXT)
The Internet and EDI. (electronic data interchange) (Technology Information)

Muiznieks, Vik
Telecommunications , v29 , n11 , p45(3)
Nov , 1995
ISSN: 0278-4831
Language: English
Record Type: Fulltext; Abstract
Word Count: 1533 **Line Count:** 00139
...for file transfer, hypertext transfer protocol (HTTP) for World Wide Web access, and telnet for remote log-ins. Each of these application protocols presents different **limitations** with respect to **use** and value-added functions such as security, encryption, and non-repudiation.

Taking mail as an example, SMTP, as defined by the Internet Engineering Task Force (IETF) standard request for comment (RFC) 822, performs the message transmission function, but only supports seven-bit American standard code for information interchange (ASCII) transmissions, **limits** the **number** of recipients, and often limits the maximum message size. Modifications to SMTP were needed to address the needs of EC/EDI. These modifications came in...

...PEM capabilities are described in RFCs 1421 to 1424, and provide for the confidentiality of messages via encryption, originator authentication, content integrity via message integrity **check** (MIC) algorithms, and non-repudiation if a **public key** mechanism is used. PGP, a privately developed public/private key system, provides mechanisms for encryption and authentication.

For EDI-based security, many companies deploy firewalls...

21/3,K/27 (Item 5 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

06716810 **Supplier Number:** 14430724 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Bob Young: vice-president, NetWare Systems Group. (NetWare 4: Q&A) (Interview)

InfoWorld , v15 , n40 , pS63(2)
Oct 4 , 1993
Document Type: Interview
ISSN: 0199-6649
Language: ENGLISH
Record Type: FULLTEXT; ABSTRACT
Word Count: 939 **Line Count:** 00077
...addition, NetWare Directory Services differ from Banyan's in the following areas:

* Flexibility. NDS can have a hierarchical tree from two levels to an unlimited **number**. Banyan has a **fixed** three-level hierarchy that cannot adjust to different organizational needs.

* Reliability. NDS is a global, distributed, and replicated database that protects against single points of...
...synchronization overhead. In larger organizations, Banyan's performance starts to degrade.

* Security. The network login and background authentication associated with NDS are secured with a **proven** industry standard **public key** technology. Banyan uses its own private token-based technology.

Q: With the ability to run application in Ring 3, can NetWare function

as an application...

21/3,K/28 (Item 6 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

05855656 **Supplier Number:** 12186859 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Vendors shouldn't profit on NIST signature standard. (National Institute of Standards and Technology, IRM Notebook) (Column)

Houser, Walter R.
Government Computer News, v11, n9, p19(1)
April 27, 1992
Document Type: Column
ISSN: 0738-4300
Language: ENGLISH
Record Type: FULLTEXT; ABSTRACT
Word Count: 983 **Line Count:** 00076
...to code the message so it is uniquely readable by the intended recipient. Only the recipient knows the private key necessary to decrypt the message.
Public-key algorithms can serve as digital signatures, ensuring the **authenticity** and integrity of messages. Messages can be "signed" by encrypting them with the sender's private key; the signature can be verified by the receiver...

...decodes properly, the receiver knows that the sender actually sent it.
The basic difference between DSS and RSA is that RSA Data Security owns the **rights** to commercial **use** of the RSA encryption algorithm. NIST has applied for a patent for the DSS algorithm, which NIST has put into the public domain, making it...

21/3,K/29 (Item 7 from file: 148)
DIALOG(R)File 148: Gale Group Trade & Industry DB

05443611 **Supplier Number:** 11180657 (USE FORMAT 7 OR 9 FOR FULL TEXT)
Finding the key to keeping records private. (ways to protect the confidentiality of electronic messages on private networks) (column)

Houser, Walter R.
Government Computer News, v10, n17, p105(1)
August 19, 1991
Document Type: column
ISSN: 0738-4300
Language: ENGLISH
Record Type: FULLTEXT; ABSTRACT
Word Count: 944 **Line Count:** 00075
...and uses that key to code the message. However, only the intended recipient should know the secret private key necessary to decrypt the incoming message.

Public-key algorithms can serve as digital signatures, ensuring the **authenticity** and integrity of messages. Messages can be "signed" by encrypting them with the sender's private key. The signature can be verified by the receiver...

...Institute of Standards and Technology is developign a public-key digital signature standard for the federal government. There already are several such techniques, but patent **restrictions** complicate their **use**
.

The holders of patent rights would expect royalty payments from commercial developers and users. Furthermore, because the recipient cannot tell from the incoming message which...

...still is looking at hashing functions to find one that complements the standard. The U.S. Postal Service has been approached to serve as a **certifying** authority for exchange of **public keys**. If USPS declines, perhaps the public telephone or data networks would step up.

NIST typically works with industry to develop national standards that then are...

V. Additional Resources Searched

Financial Times FullText (via ProQuest): No relevant results.

Internet & Personal Computing Abstracts (via EBSCOhost): No relevant results.